DISTRIBUTED SNIFFER SYSTEM™

Expert Analyzer Operations Manual

NETWORK GENERAL CORPORATION

DISTRIBUTED SNIFFER SYSTEM™

Expert Analyzer Operations Manual

Network General

NETWORK GENERAL CORPORATION

DISCLAIMER OF WARRANTIES

The information in this document has been reviewed and is believed to be reliable; nevertheless, Network General Corporation makes no warranties, either expressed or implied, with respect to this manual or with respect to the software and hardware described in this manual, its quality, performance, merchantability, or fitness for any particular purpose. The entire risk as to its quality and performance is with the buyer. The software herein is transferred "AS IS."

Network General Corporation reserves the right to make changes to any products described herein to improve their function or design.

In no event will Network General Corporation be liable for direct, indirect, incidental or consequential damages at law or in equity resulting from any defect in the software, even if Network General Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Document prepared by Sid Heaton with contributions from Jim Mar, Terri FitzMaurice, and Arlene Brenner.

March 1993

P/N:20103-001

Table of Contents

List of Figures

Chapter 1. Overview—What a Sniffer Analysis Server Does

Chapter 2. Getting Familiar with the Expert Analyzer

Chapter 3. Expert Analyzer Options

Chapter 4. Expert Analyzer Capture and Display

List of Procedures

Chapter 1. Overview—What a Sniffer Analysis Server Does

Chapter 2. Getting Familiar with the Expert Analyzer

Chapter 3. Expert Analyzer Options

Chapter 4. Expert Analyzer Capture and Display

PREFACE

Preface

About This Manual

This manual describes the functions and operations of the Expert Sniffer® analyzer, a software application of the Distributed Sniffer System™ (DSS). It also provides recommendations on how to use the Expert analyzer effectively to detect and solve network problems. This manual describes only those operations relating to the Expert mode of the analysis application. For information on Classic mode operations, see the *Distributed Sniffer System: Analyzer Operations Manual.*

The Distributed Sniffer System consists of two types of product: Sniffer Servers and SniffMaster™ Consoles. Each Server observes the local or wide area network to which it is attached; Consoles control Servers and display the results of the Servers' activities.

Manuals for the Distributed Sniffer System

Two types of manuals accompany the Distributed Sniffer System. The primary manuals, which include this one, describe the system's normal operations; the supplementary manuals describe the programs that configure and test the system's various hardware and software components. The actual manuals in your shipment depend on the system configuration.

Figure i lists the primary manuals for the Distributed Sniffer System

For Information On...	Read...
Installing and configuring Servers and Consoles. Operating Consoles.	*Distributed Sniffer System: Console Installation and Operations Manual, Server Installation and Operations Manual, or Sniffer Server Installation Note.*
Operating the Server's Analyzer functions on an Ethernet, token ring, or wide-area network.	*Distributed Sniffer System: Analyzer Operations Manual.*
Operating the Server's Expert Analyzer functions on an Ethernet, token ring, or wide area network.	*Distributed Sniffer System: Expert Analyzer Operations* (this manual).
Operating the Server's Monitor functions on a token ring network.	*Distributed Sniffer System: Token Ring Monitor Operations Manual.*
Operating the Server's Monitor functions on an Ethernet network	*Distributed Sniffer System: Ethernet Monitor Operations Manual.*
Various network and protocol types.	*Distributed Sniffer System: Network and Protocol Reference Manual.*

Figure i. Primary manuals for the Distributed Sniffer System.

Figure ii lists the supplementary manuals for the Distributed Sniffer System.

For Information On...	Read...
IBM 16/4 token ring adapter (ISA)	*Token Ring 16/4 Network Guide to Operations*
IBM 16/4 token ring adapter (MCA)	*Token Ring 16/4 /A Network Guide to Operations*
InterLan NI5210 Ethernet controller (ISA)	*NI5210 Installation Manual*
InterLan NI9210 Ethernet controller (MCA)	*NI9210 Installation Manual*
4-Port Serial Adapter (ISA)	*QS-100D Installation Manual*
4-Port Serial Adapter (MCA)	*QS-1000 Installation Manual*

Figure ii. Supplementary manuals for the Distributed Sniffer System.

If the product shipment includes release notes or README files on disks, the information in the notes or files supersedes the information in this and other manuals.

Audience of This Manual

This manual has been prepared with the following assumptions:

- You are a network manager or troubleshooter who understands how networks operate.
- You are familiar with DOS.

Organization of This Manual

Figure iii describes the organization of this manual.

Chapter/Appendix	Contents
Chapter 1, "Overview-What a Sniffer Analysis Server Does"	Provides an overview of the Distributed Sniffer System and describes its capabilities. Also defines key terms, lists new functions, and provides an introduction to the user interface.
Chapter 2, "Getting Familiar with the Expert Analyzer"	Provides an overview of the Expert Sniffer analyzer and describes its capabilities. Also defines key Expert terms, and lists new functions.
Chapter 3, "Expert Analyzer Options"	Describes various Expert analyzer precapture options, including a description of the Expert layers, how to set an Expert threshold, and how to set an Expert trigger.

Figure iii. Scope of each chapter or appendix in this manual.

Chapter/Appendix	Contents
Chapter 4, "Expert Analyzer Capture and Display"	Describes all Expert screen displays. Provides information on how to navigate through the Expert displays to get the maximum information about network problems.
Appendix A, "Symptom and Diagnosis Messages"	Provides a list of solutions to common problems.

Figure iii. Scope of each chapter or appendix in this manual.

Navigational Aids Used in this Manual

This manual uses icons in the margin to help you locate important information as explained below:

IMPORTANT INFORMATION. Next to this icon is information that is especially important; you should be certain to read it carefully before you proceed. This icon also indicates useful and valuable ways to use the product.

CAUTION. Next to this icon is information that you must know to avoid damage to data files, program files, or hardware devices. This icon also indicates information that you must know to avoid possible injury to yourself or others.

PROCEDURE. Next to this icon is a series of steps for accomplishing a particular task.

To help you find procedures easily, a separate List of Procedures is provided in this manual in addition to the Table of Contents and List of Figures.

Conventions Used in This Manual

Special Notations

The following describes the conventions used in this manual:

Bold

Menu options and menu listings are in bold type. Two examples follow:

Move to **Display**, and press Enter.

To set a display filter, move to **Display\Filters** and use the spacebar to toggle the desired filter.

UPPERCASE

Filenames and commands you type at a DOS prompt are in uppercase. For example:

Modify the AUTOEXEC.BAT file if necessary. To duplicate the file, use the COPY command.

Bold italics Variables for which you insert values are in bold italics. For example:

Type the number of minutes and seconds in the ***mm:ss*** format.

`Screen font` Screen messages are printed in monospaced font. For example:

If a monitoring session is in progress, the following message appears:

```
You must stop monitoring before you can use this feature.
```

Terminology

Hexadecimal numbers in the manual are followed by "(hex)"; numbers without any notations are decimal. For example, "The maximum number of stations is 75. The default memory address is D8000 (hex)."

The terms "monitor" and "analyzer" refer to software applications that run on token ring or Ethernet Sniffer Servers. The term "Console" refers to control and display software running on a dedicated PC.

This manual sometimes uses abbreviated names for the various components of the Distributed Sniffer System. The term "analyzer" stands for the analysis application. The term "Expert analyzer" stands for the analysis application capturing or displaying in the Expert window.

Screen Displays and Keyboard Input

Enter all the keystrokes mentioned in the manual from the SniffMaster Console. Similarly, all the screen displays generated by a Server appear on the Console's screen.

The screen displays in this manual serve mainly as examples and may not be identical to the ones you see on your Console screen. For example, you can choose to have the Console show the Server name on each monitor display, but the screens in this manual do not show the name.

Other Sources of Information

Network General Corporation (NGC) provides other sources of information that can help you become familiar with the Distributed Sniffer System.

On-Line Help

After highlighting an item in a Console, Analyzer, or Monitor menu, you may notice a phrase or sentence in a panel near the bottom of the screen. It explains the meaning of the highlighted item.

When running an analyzer application, there are two kinds of on-line help. If you want to obtain general information on a particular feature of the analyzer application, press F1(**Help**) whenever its key label appears on the screen. A window containing a list of topics opens. Note that in the Expert window, the key label for F1 reads **Explain**. Explain screens provide context-sensitive solutions to specific network problems highlighted in the Expert window. Help screens provide general descriptions and instructions for the items in the analyzer's menus.

Technical Support

The toll-free number for obtaining technical support for the Distributed Sniffer System is listed below. Before calling, however, please check the Troubleshooting Guide in the *Distributed Sniffer System: Analyzer Operations* manual. You will find tips for troubleshooting your system before requesting help as well as information you will need to provide if you do request help.

Phone for Network General's Technical Support Department:	(800) 395-3151
FAX	(415) 327-9436

Training

NGC offers a comprehensive set of training courses focused on hands-on network analysis and troubleshooting using the Expert Sniffer Network Analyzer. For more information, contact your sales representative.

CHAPTER ONE: OVERVIEW—WHAT A SNIFFER ANALYSIS SERVER DOES 1

Overview—What a Sniffer Analysis Server Does

Overview

This chapter provides a general orientation to the Sniffer analysis Server. The chapter starts with a general description of the distributed analysis system and its components: SniffMaster *Consoles*, Sniffer *monitor Servers*, Sniffer *analysis Servers*, and Sniffer *combined monitoring and analysis Servers* (combining the functions of monitoring and analysis in a single Server).

The chapter depicts the organization of a Server's *analysis* functions by showing a map of the way information flows between them and back to the Console. Analysis has two main phases: *capture* (when frames are recorded in a storage buffer), followed by *analysis* (when the captured frames are interpreted and displayed). Capture can occur *live* from the network, or as a *replay* of previously captured data.

This manual describes the operation of the analysis application in Expert mode. For information on operating the analysis application in Classic mode, or information on the analyzer in general, see the *Distributed Sniffer System: Analyzer Operations Manual.*

The Distributed Sniffer System

The Sniffer analysis Server whose operations are described in this manual is one of the principal components of the Distributed Sniffer System. For a perspective on the entire system and the role of the SniffMaster Console in controlling it, see the companion publication, *Distributed Sniffer System: Console Installation and Operations Manual.*

About the Distributed Sniffer System

A Distributed Sniffer System consists of *SniffMaster Consoles* controlling network monitoring and analysis tools known as *Sniffer Servers.* A basic Distributed Sniffer System is illustrated in Figure 1–1.

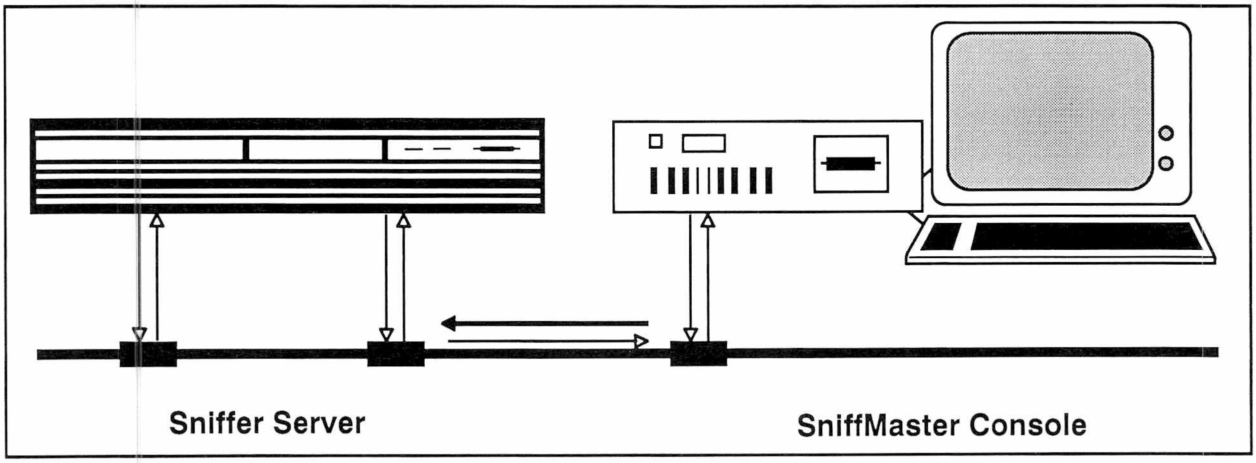


Figure 1–1. Basic Distributed Sniffer System components.

SniffMaster Console

Consoles connect to Servers and allow you to observe your network and control the Servers' activities. Consoles use proprietary software for communicating with Servers.

Sniffer Servers

Servers are computers with proprietary software and hardware. They use two cards: a Transport Card that supports communication with Consoles and a *Monitor Card* that uses software to capture frames and collect statistics from the network.

DSS Software

SniffMaster Consoles receive network information from Servers which use monitoring and/or analysis software applications.

The monitoring application maintains a set of real-time counters, charts, and summaries of network activity. The monitor transmits alarms to Consoles based on user-specified threshold values.

The analysis application captures network traffic in two modes.

- Classic capture. Classic capture records network traffic for later interpretation.
- Expert capture. While capturing in Expert mode, the analyzer alerts you to symptoms and diagnoses as it captures traffic. Symptoms and diagnoses represent potential network problems detected by the analyzer. In this mode, alarms are sent to the Console when diagnoses become active.

This manual describes the operation of the analysis software application in Expert mode. For information on capturing in Classic mode, or general information on the analysis application, see the *Distributed Sniffer System: Analyzer Operations* manual. For information on the monitoring application, see the *Distributed Sniffer System: (Ethernet or Token Ring) Monitor Operations Manual.*

Major Components of the Sniffer Analysis Server

The Sniffer analyzer —that is, the network analyzer program installed in a Sniffer analysis Server— is a software component of the Distributed Sniffer System. Figure 1–2 summarizes the major software components of a Sniffer analysis Server.

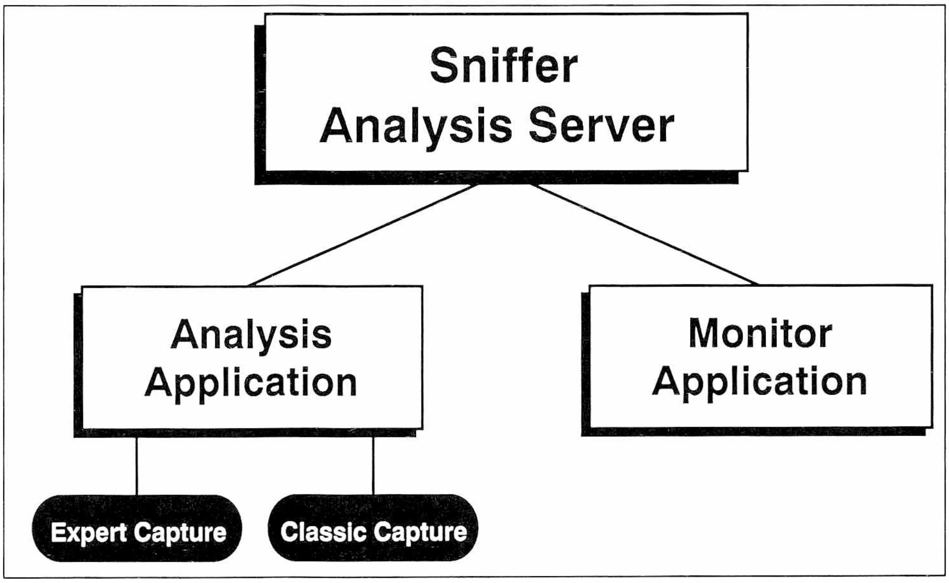


Figure 1–2. Major software components of a Sniffer analysis Server.

You can operate the analysis application in either Expert or Classic mode. When this manual mentions the "Expert Sniffer analyzer," it is referring to the analysis application capturing or displaying in Expert mode. Similarly, the term, "Classic Sniffer analyzer," refers to the analysis application capturing or displaying in Classic mode.

The Role of the Analyzer

An analyzer records and interprets network transmissions. The work of the analyzer occurs in two main stages:

Capture The analyzer records network traffic for later interpretation. Capture can be filtered to record only traffic that meets certain criteria. Capture can be frozen when a user-definable trigger event occurs. This assures that the retained capture buffer includes traffic just before or after the event of interest.

During capture in Expert mode, frames are analyzed as they are stored in the buffer. Alarms may be generated and sent to the Console while in capture mode. The various Expert displays are dynamically updated as capture proceeds, allowing you to navigate between various levels of detail to solve network problems in real time.

While capturing frames, the analyzer software maintains and displays graphs or tables that summarize recorded traffic.[1]

Display The analyzer interprets the recorded traffic. In the Classic window, the analyzer decodes the various layers of protocol in the recorded frames and displays them as English abbreviations or summaries. The analyzer can filter the display to show only those frames that meet certain criteria.

You can also display the captured frames in the Expert window, allowing you to investigate the symptoms and diagnoses the Expert analyzer detected. In the Expert window, all the views available during capture are also available during display. You can toggle display between the Classic and Expert windows by pressing the function key F3.

The Analyzer as (Mostly) Passive Observer

A Sniffer Server "hears" all traffic that passes over the segment it is observing. On a WAN/Synchronous link, it hears traffic in both directions ("from DTE" and "from DCE"). On a LAN, it hears all traffic that passes over the segment or subnet that it is monitoring. It is characteristic of a LAN that every station physically receives every transmission. Ordinarily, each station ignores all messages except broadcast messages and those addressed to it. The analyzer not only hears all transmissions, but, while in "capture" mode, it can record them, regardless of how they're addressed.

In general, the Sniffer Server observes, tabulates, analyzes, or captures, but contributes no traffic to the network it is observing. However, when the analyzer is observing a LAN, it may contribute to the LAN's traffic as follows:

- On Ethernet and token ring, an analyzer can generate test frames. In this buffer mode, it repeatedly transmits the single test packet you specify or a file of captured frames.
- On Ethernet, the analyzer can emit a pulse to test for cable defects.By default, the Ethernet analyzer emits a single test frame (as part of a time domain reflectometer test) just prior to starting capture. The analyzer does this to determine whether or not it is attached to an Ethernet cable. On some networks, this may be disruptive. If so, you can disable this feature in the Options menu of the analyzer. See the *Distributed Sniffer System: Analyzer Operations Manual* for more information.

[1] The analyzer's displays during capture resemble some of the displays produced by the monitor. Don't confuse this mini-monitoring during capture with the full-blown monitor application, which is separate.

- On token ring, every station must participate in the ring by forwarding buffer mode traffic from its upstream neighbor to its downstream neighbor. The analyzer does that in the same way as other stations. However, the analyzer does not reply to the poll for standby monitors, and never acts as the ring's active monitor. It is thus invisible to most other stations.

  Note: During traffic generation, however, the token ring analyzer may act as the active monitor if no other station is transmitting and responds to standby monitor polls.

- On token ring, the analyzer periodically transmits a frame addressed to "LAN Manager" announcing "trace tool present." If properly configured, the LAN Manager can force such a station to leave the ring immediately.

A Map of the Analyzer's Functions

The analyzer's activities are divided into the set of functions described below. The diagram in Figure 1–3 represents schematically the route by which information flows between the various functions. Following the path of the frames as they are captured, they are affected by the analyzer's principal functions as follows:

- Capture filters determine which frames are discarded and which are captured.
- Capture views show the capture's progress, in Expert, individual stations, pair counts, or skyline formats.
- Trigger detector scans arriving frames for a user-defined pattern or event. When it detects this pattern or event, it stops capture so that frames preceding or following the event are retained and writes the frames to disk.
- Capture buffer is the storage area for frames that have been accepted. From here they are subsequently interpreted and displayed.
- Object database is the storage area for Expert information, such as network objects, symptoms, and diagnoses.
- Protocol interpreters identify the protocols nested within each frame and interpret their contents.
- Display filters determine which frames in the capture buffer are displayed.
- Frames that pass the display filters can be displayed in three views:

  — Summary

  — Detail

  — Hex with ASCII or EBCDIC

Output of the display can be saved to a file, sent to a printer, or imported into spreadsheets.

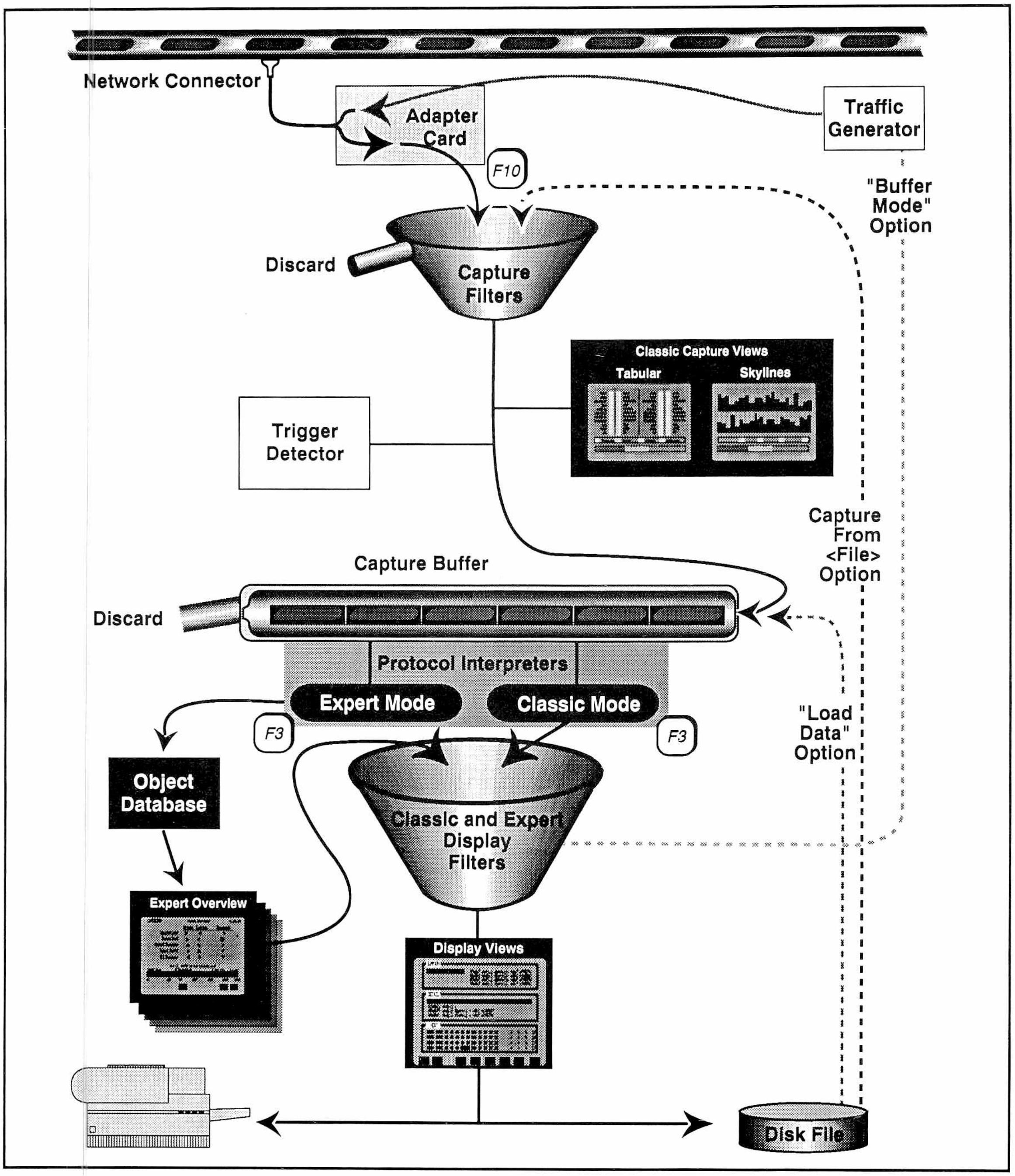


Figure 1–3. Overview of Sniffer analyzer functions.

The Analyzer's Menus and Controls

While you operate a Sniffer analyzer, you're always working from a SniffMaster Console. There are menus to operate the Console and menus to operate the individual Servers. From the SniffMaster Console menus, you activate the connection to one or more Servers.

What You See When You Connect to a Server

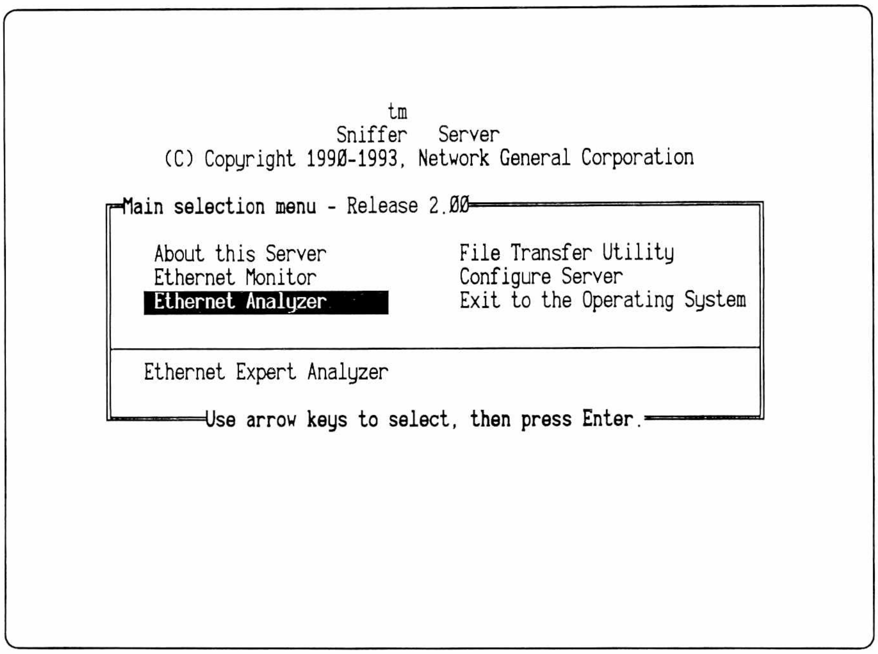
When you display a Server's screen, you are observing what the Server is doing at the moment. Note that the Server was operating before you connected to it and that it will continue operating after you disconnect from it. The Server can continue operating whether or not you choose to display its screen at your Console.

If the analysis Server has been collecting data unattended, you see the display that was last requested, updated to show the current situation. If the analysis Server has been started but given no specific instructions, you see its initial selection menu. If an earlier instruction exited from the Server's menus and returned to DOS, you see the DOS prompt.

The Server's Selection Menu

When the analysis Server is newly installed, or whenever it has just been reset or powered up, upon connection you'll see its *main selection menu*. From the selection menu, you can tell the Server to run the Sniffer *monitor* or the Sniffer *analyzers*. You may also select the file transfer utility or you may decide to configure the Server.

In Figure 1–4, the selection menu lists the major choices available to you. (The items in the menu depend on the configuration of your particular Sniffer Server.)



```
                         tm
                    Sniffer   Server
        (C) Copyright 1990-1993, Network General Corporation

 Main selection menu - Release 2.00

    About this Server              File Transfer Utility
    Ethernet Monitor               Configure Server
    Ethernet Analyzer              Exit to the Operating System

   Ethernet Expert Analyzer

          Use arrow keys to select, then press Enter.
```

Figure 1–4. Server selection menu.

In each menu, one item is *highlighted.*[1] The lower portion of the panel contains a brief explanation of the highlighted entry. Pressing one of the cursor keys moves the highlight to another entry. To execute the entry that's highlighted, press Enter.

To start an analyzer

1. From the SniffMaster Console, connect to a Server. (For details regarding this step at the Console, see the *Distributed Sniffer System: Console Installation and Operations Manual.*)

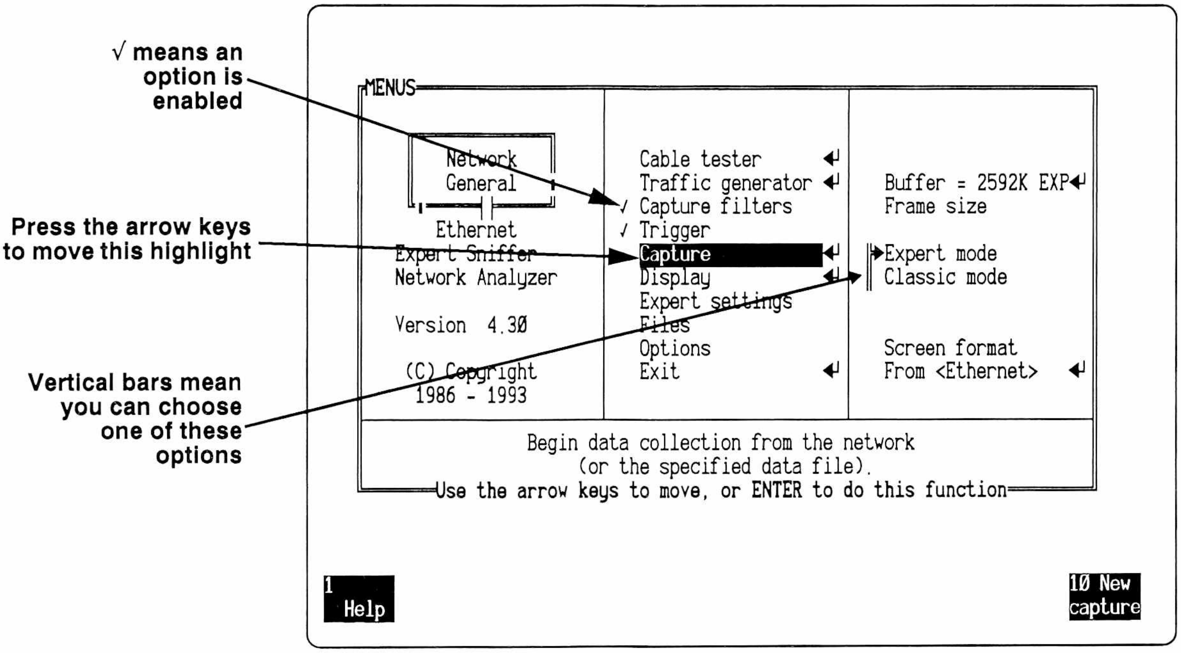
   Result: You see the Server's current screen. When the Server has been newly installed or has been reset, you'll see its main selection menu.

2. In the Server's main selection menu, move the highlight to the analyzer you want and press Enter.

Tree-Structure of the Analyzer's Menus

The Sniffer analysis Server is entirely controlled from menus presented on the screen of the SniffMaster Console. When you choose to run an analyzer, control passes immediately to the analyzer's main menu. An example (for an Ethernet analyzer) is shown in Figure 1–5.

[1] We use "highlight" to mean the distinctive display of the selected item at the center of the screen. Depending on the type of display you're using, this may be in a contrasting color, or flashing, or in reverse video.



√ means an option is enabled

Press the arrow keys to move this highlight

Vertical bars mean you can choose one of these options

```
MENUS
  Network              Cable tester      ↵
  General              Traffic generator ↵   Buffer = 2592K EXP↵
                     √ Capture filters       Frame size
  Ethernet           √ Trigger
Expert Sniffer         Capture           ↵   ▶Expert mode
Network Analyzer       Display           ↵   Classic mode
                       Expert settings
Version  4.30          Files
                       Options               Screen format
  (C) Copyright        Exit              ↵   From <Ethernet>   ↵
  1986 - 1993
               Begin data collection from the network
                     (or the specified data file).
       Use the arrow keys to move, or ENTER to do this function

1                                                        10 New
 Help                                                    capture
```

Figure 1–5. Main menu of the Sniffer analyzer (in this case, for Ethernet).

All Sniffer analyzer menus have the same structure. While details vary according to the network and protocol interpreter suites installed, the organization is the same. The entire menu is a tree, with its root (the main menu) to the left and its branches and leaves to the right. Only a part of the menu is visible at a time. Using the cursor keys, you move a window over the menu. Since the window is fixed on the screen, the menu appears to move under the stationary window.

When the menu is active, the screen shows three panels side-by-side. You control the center panel. Within that center panel, the center row is highlighted. That is your location on the menu. When you first start a Sniffer analyzer, the center panel lists the alternatives available from the root of the tree. Some alternatives appear above the highlight, some below it. Initially, the highlight is on Capture.

When you press the Cursor Up key, the highlight appears to move, and the item above Capture becomes highlighted. The highlight doesn't really move; instead, the entire center panel scrolls downward so that the (stationary) highlight is now on the row above. Alternatively, to jump directly up or down to a particular item, you may type the first letter of its name. The highlight jumps to the next item beginning with that letter.

The panel to the right shows choices in the submenu that are associated with the item highlighted in the center panel. As soon as you bring a different item to the center highlight, the entire right panel changes. The right panel always shows the submenu that goes with the item that's highlighted in the center (see Figure 1–6).

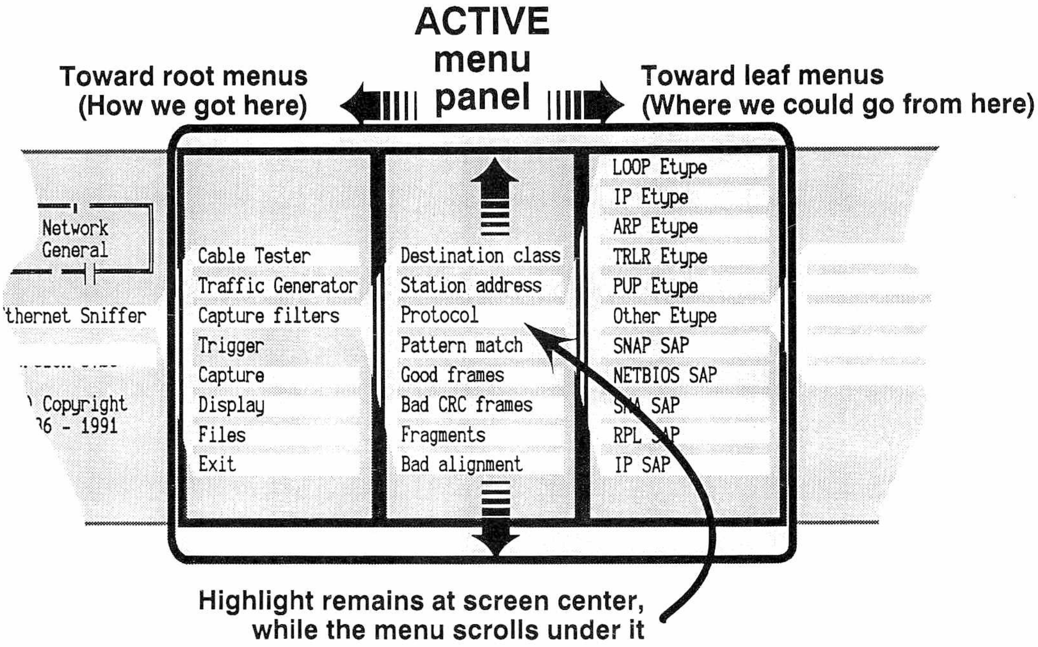


Figure 1–6. Scrolling over the tree-structured menu.

To work with the Sniffer analyzer menus:

1. Press one of the four arrow keys to move the highlight to the desired menu item. Note that any options associated with that item appear in the panel to the item's right. As you move the highlight, the relevant options are displayed, while those associated with another option disappear.

2. For options followed by a ↵ symbol, pressing Enter when the option is highlighted either executes the command or it displays a listing or dialog box. From this display, you can either choose an option or enter information. In Figure 1–5, for example, pressing Enter when the **From <Ethernet>** option is highlighted results in a listing of files from which you can choose one as the capture source.

3. For options connected by a vertical bar (radio control), you can choose an option by moving the highlight to that option and pressing Spacebar. All other options connected by the bar are automatically disabled. In the main menu, for example, you can choose between capturing in **Classic mode** or in **Expert mode**.

   Note: A radio control is so called because– like an old-fashioned radio control– selecting one option deselects all others.

4. For options preceded by √ or x symbols, you can enable or disable those options by moving the highlight to them and pressing Spacebar. Any such options are always either enabled (√) or disabled (x); pressing Spacebar toggles between the two states.

Features of the Expert Sniffer Analyzer

Figure 1–7 outlines some of the features provided by the Expert analyzer.

Global statistics display	The Expert analyzer provides statistics detailing the percentage composition of network traffic by protocol family. You can tell, at a glance, how much of your network's traffic is TCP/IP, how much is DECnet, and so on.
Expert analysis during capture	The Expert analyzer can analyze network traffic and generate diagnostic messages while capturing frames from the network or a file. It can also capture traffic in Classic mode and then perform Expert analysis on the frames in the capture buffer later.
Explain screens	In the Expert window, you can pause capture and press F1 to show a detailed context-sensitive Explain screen pertaining to a symptom, diagnosis, or network object that is highlighted.
Multiple-layer analysis	The Expert analyzer can analyze problems at the Application, Connection, Network Station, and Data Link layers. On a token ring network, it can also analyze problems at the Medium Access Control (MAC) layer. You can specify that the analyzer perform Expert analysis on only those layers that interest you.
Expert triggers	You can specify one or more network events as trigger events. For example, you can configure the analyzer to stop capturing immediately after detecting a duplicate network address.
Network object filters	After capture, you can automatically filter out frames that are irrelevant to a particular symptom, diagnosis, or network object. After filtering, the analyzer displays only those frames related to the selected object, making it easy for you to concentrate on one problem at a time.
Display with symptoms	You can elect that the Classic data display window show a one-line description of any symptom associated with a frame.
Filter on symptoms	You can elect to display only those frames exhibiting symptoms.

Figure 1–7. New features of the Expert Sniffer analyzer.

The following chapters describe each of these features in detail.

CHAPTER TWO: GETTING FAMILIAR WITH THE EXPERT ANALYZER 2

Network General

Getting Familiar with the Expert Analyzer

Overview

This chapter defines key Expert analyzer concepts, gives instructions on how to start the Sniffer analyzer in Expert mode, and describes how to navigate among the Expert analyzer screen displays. The chapter gives you a "feel" for how the Expert analyzer operates, but does not discuss in detail the various features of the analyzer. The screens in this chapter are samples that illustrate the effects of various steps; you might see different messages on your analyzer as you follow the instructions.

Remember that the Sniffer analyzer can capture in either Expert or Classic mode. The manual will sometimes make reference to the ***Expert analyzer***. It should be understood that this means the Sniffer analyzer capturing or displaying in its Expert mode.

This chapter assumes that you have successfully set up your Distributed Sniffer System, attached the analysis card to the network, and displayed the Main Selection Menu. If you have not done so, refer to the *Distributed Sniffer System: Console Installation and Operations Manual* and the *Distributed Sniffer System: Server Installation and Operations Manual* for information on getting started with the Distributed Sniffer System.

Expert Analyzer Terminology

When you start capture in Expert mode, the analyzer immediately begins constructing a database of *network objects* from the traffic it sees. The Expert analyzer uses its real-time protocol interpreters to learn about all the network stations, routing nodes, subnetworks, and connections related to the frames in the capture buffer. Using this information, the Expert analyzer can detect and alert you to potential problems that may be plaguing the network. The analyzer categorizes network problems as being either *symptoms* or *diagnoses*. Network objects, symptoms, and diagnoses are defined below.

About Network Objects

The amount of raw data on a given network can be quite immense. By performing multilevel protocol analysis on the frames that pass through its real-time protocol interpreters, the Expert analyzer extracts a small number of network objects from the huge amount of information it processes.

Network objects can be any of the following:

- A DLC station
- A network station
- A connection
- An application

- A subnetwork

The Expert analyzer learns about the network to which it is attached by intelligently correlating the various network objects it creates.

About Symptoms

When the Expert Sniffer analyzer detects an abnormal or unusual network event, it considers such an event a "symptom" indicative of a possible network problem. The analyzer displays a symptom message in one of the Expert windows.

After establishing an accurate network baseline, experienced users can alter the Expert thresholds to modify what constitutes a symptom. That is, you can specify that a certain network parameter (for example, the number of identical requests sent by an application) must exceed a certain limit before the analyzer displays a symptom message. (For information on setting thresholds, see "Setting Thresholds for Symptoms and Diagnoses" on page 3–13.)

About Diagnoses

In addition to revealing symptoms, the analyzer also uncovers "diagnoses." There are two types of diagnoses:

- A diagnosis caused by several symptoms or recurrences of a symptom. As a symptom becomes more severe, the analyzer concludes that the symptom is not only an indicator but also a problem in itself.

  For example, if network traffic increases suddenly over a short period of time, the Expert analyzer may alert you to a **LAN overload** symptom. If the **LAN overload** symptom persists over a longer period of time, the analyzer will display a **LAN overload** diagnosis. You can define thresholds for this type of diagnosis. For example, you could specify that a **LAN overload** diagnosis be generated whenever a **LAN overload** symptom is active for more than 20 percent of a minute.

- A diagnosis caused by a single network event that is itself considered to be problematic. The analyzer immediately assumes that the event represents a problem; there are no user-defined thresholds.

  For example, when the Expert analyzer detects two stations with the same network address, it will immediately display the symptom and diagnosis **Duplicate network address**. There is no threshold to exceed.

About Alarms

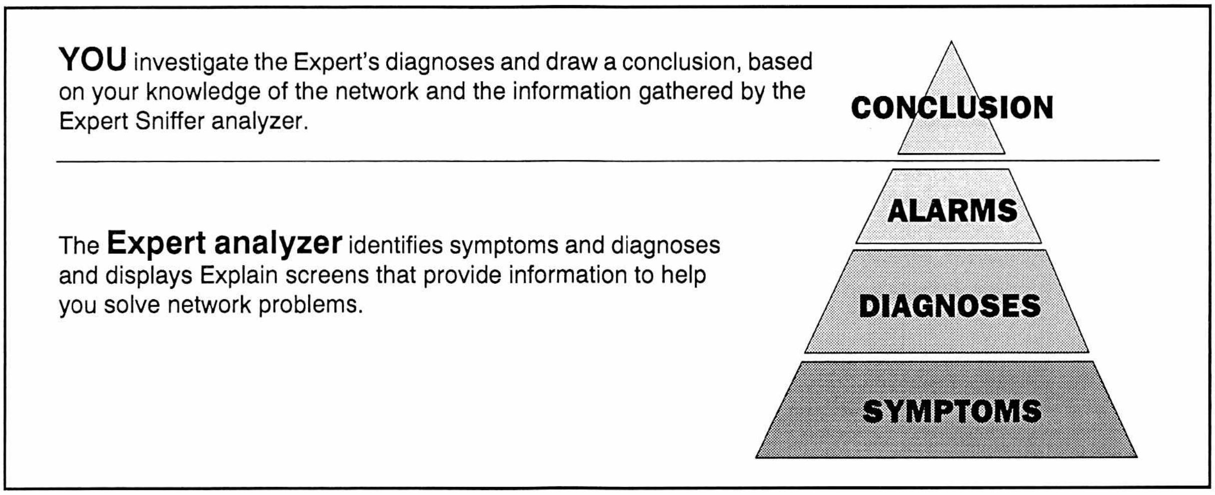
An alarm is a message sent to a Console to make an entry in the Console's Alarm Log. An Expert alarm is derived from a diagnosis in such a way that the alarm fields convey information about the condition and lead you to more detailed diagnosis information on the Server that generated the alarm. The alarm does not replace the Expert diagnosis display on the Server.

Each time a diagnosis is activated or reactivated after being closed, an alarm may be sent. The actual rate at which alarms from a diagnosis are sent is determined by the **Expert settings\Throttle** setting. The default is one alarm per minute, which means for the Server to "send no more than one alarm per minute from a single diagnosis." No alarm is generated when a diagnosis is either updated or closed.

Alarms sent by an Expert Server display the following information on the Console's Alarm Log:

- **Alarm Priority**: Set as configured on the Expert Server.
- **Timestamp**: The most recent time the diagnosis on the Expert Server went into the active state.
- **Offender**: This field is not set by Expert. Because alarms generated by the Expert Server may have their origins in more than one node, it is not always possible to assign a single offender address to an alarm. Each alarm will contain relevant addresses within its descriptive text while the offender field remains empty.
- **Alarm Type Description**: the text that appears on the **Diagnosis Summary Screens** of the Expert Server.

The Expert analyzer uncovers symptoms and provides diagnoses. You draw a conclusion based on the information gathered by the analyzer and your knowledge of the network. Figure 2–1 summarizes the role of the Expert analyzer in solving network problems.



YOU investigate the Expert's diagnoses and draw a conclusion, based on your knowledge of the network and the information gathered by the Expert Sniffer analyzer.

The **Expert analyzer** identifies symptoms and diagnoses and displays Explain screens that provide information to help you solve network problems.

Figure 2–1. Role of the Expert analyzer in solving network problems.

Starting the Sniffer Analyzer in Expert Mode

Network General provides the Expert Sniffer Analyzer application with a set of default Expert thresholds that determines under what conditions the Expert analyzer will indicate various network problems. These default settings make the Expert analyzer a turnkey application requiring little or no configuration.

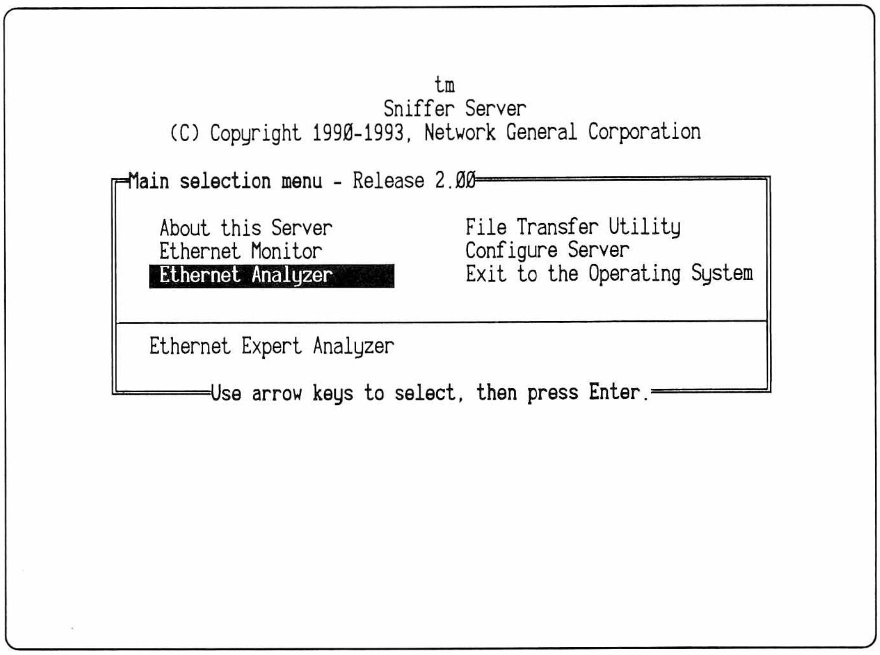
This section describes how to start the Expert analyzer capturing with the default settings. There are other ways to run the Expert analyzer; the following procedure is just one of them. Chapters 3–4 describe how to customize a capture session.

To start capturing and analyzing frames in Expert mode:

1. From the SniffMaster Console, connect to an analysis Server which has the Expert Sniffer Analyzer software loaded. For information on connecting to Servers from the SniffMaster Console, refer to the *Distributed Sniffer System: Console Installation and Operations Manual.*

   Result: If connection is successful, the Main Selection Menu of the Sniffer Server appears. Figure 2–2 is similar but may not be identical to the Main Selection Menu on your Sniffer Server.

   Note: The screens shown in this example are from an Ethernet analyzer. However, the procedure is the same for any other network type.

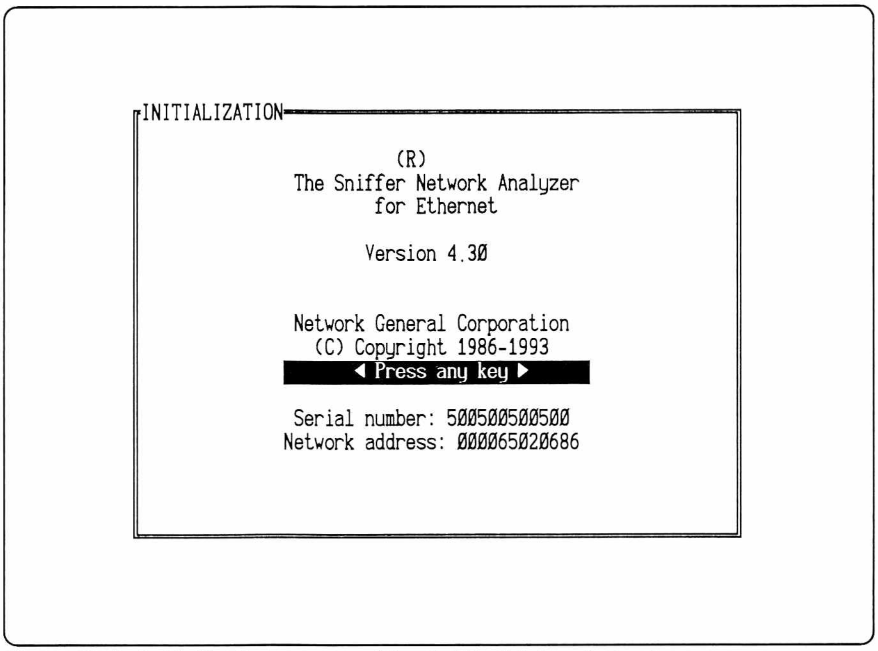


```
                              tm
                        Sniffer Server
          (C) Copyright 1990-1993, Network General Corporation

   Main selection menu - Release 2.00

     About this Server              File Transfer Utility
     Ethernet Monitor               Configure Server
     Ethernet Analyzer              Exit to the Operating System

    Ethernet Expert Analyzer

           Use arrow keys to select, then press Enter.
```

Figure 2–2. Main Selection Menu of a Sniffer Server.

2. Using the cursor keys, highlight the **Analyzer** menu option, and press Enter.

   Result: The Sniffer analyzer application is loaded into RAM. When initialization completes, the system will display a screen similar to Figure 2–3.



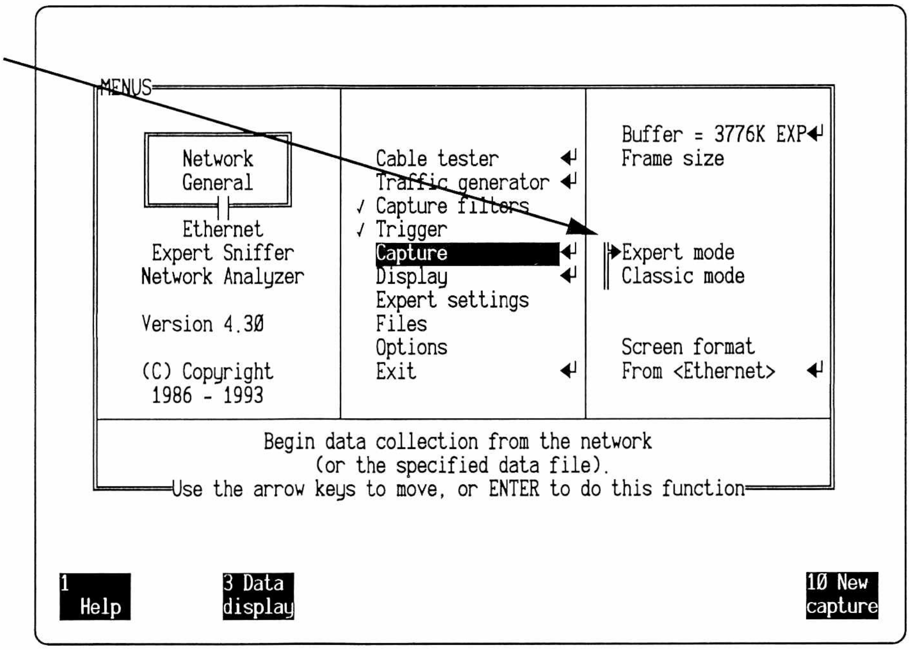
```
INITIALIZATION
                    (R)
        The Sniffer Network Analyzer
               for Ethernet

               Version 4.30


         Network General Corporation
          (C) Copyright 1986-1993
            ◀ Press any key ▶

        Serial number: 500500500500
       Network address: 000065020686
```

Figure 2–3. Initialization screen of the Sniffer Network Analyzer.

3. Press any key.

   Result: The Main Menu of the Sniffer analyzer appears. From this menu you can control all Classic and Expert analyzer functions. Figure 2–4 shows the Main Menu of the Sniffer analyzer.

Capture mode selection (currently in Expert mode).



```
Begin data collection from the network
      (or the specified data file).
Use the arrow keys to move, or ENTER to do this function
```

Figure 2–4. Main Menu of the Sniffer analyzer (in this case, for Ethernet).

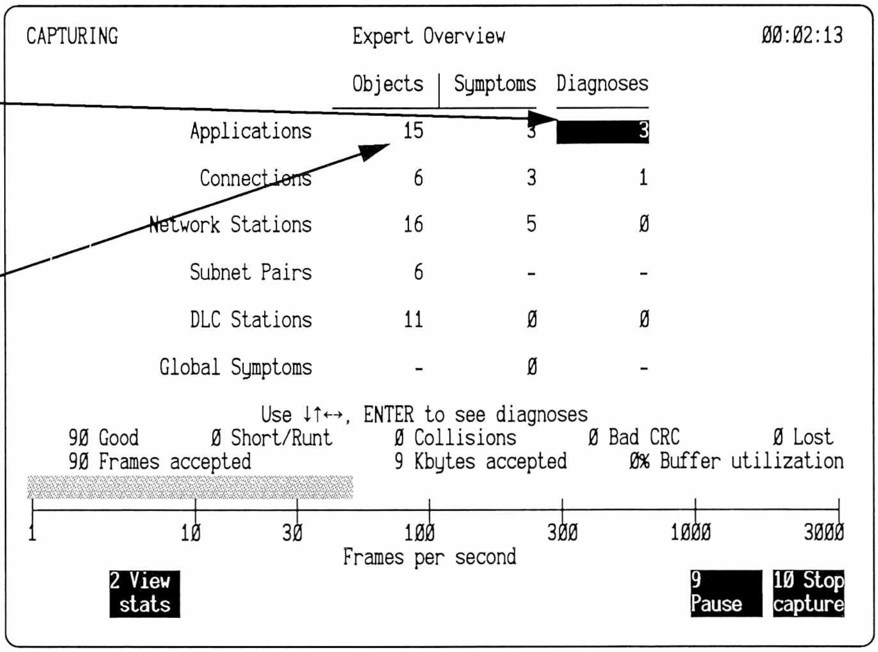
When you start the Sniffer analyzer from the Main Selection Menu, it automatically defaults to Expert capture mode. Note that the pointer in the far right panel of Figure 2–4 points to **Expert mode** rather than **Classic**. For information on capturing in Classic mode, see the *Distributed Sniffer System: Analyzer Operations* manual.

4. Press F10 (**New Capture**) to start capture. Alternatively, you can use the cursor keys to highlight **Capture** and press Enter.

   Result: The analyzer begins capture in Expert mode. The Expert Overview appears (Figure 2–5), displaying the results of Expert analysis as it captures frames.

Diagnosis count column. Notice that the analyzer has already made three diagnoses at the Expert Application layer.

Network object counters. The analyzer has detected 15 objects at the Expert Application layer. See page 2–3 for a definition of network objects.



```
CAPTURING                        Expert Overview                    ØØ:Ø2:13

                               Objects | Symptoms  Diagnoses

             Applications        15        3           3

              Connections         6        3           1

         Network Stations        16        5           Ø

             Subnet Pairs         6        -           -

             DLC Stations        11        Ø           Ø

           Global Symptoms        -        Ø           -

                    Use ↓↑↔, ENTER to see diagnoses
  9Ø Good        Ø Short/Runt      Ø Collisions      Ø Bad CRC        Ø Lost
  9Ø Frames accepted               9 Kbytes accepted    Ø% Buffer utilization
```

Figure 2–5. Expert Overview window of the Expert analyzer.

Notice that in Figure 2–5 the Diagnoses column already indicates three diagnoses made at the Expert application layer. The Expert analyzer has uncovered problems on your network based on the symptoms and network objects it has detected. You can decide whether you want to see the diagnoses and further investigate the cause of these problems.

The analyzer categorizes network problems according to the Expert layer at which they occur. Expert layers have a rough parallel in the OSI model. For a complete description of how the Expert model of the network compares to the OSI model, refer to "Expert Layers and the OSI Model" on page 3–4.

About the Expert Window

Once capture in Expert mode begins, you are in the *Expert window*. The term *Expert window* refers to the set of available Expert screen displays in which you can view the results of Expert analysis. In general, the following types of Expert screen displays are available in the Expert window.

- Overview
- Summary

- Detail
- Statistics

These screens vary depending on many factors; this chapter describes several. For a complete description of all displays available in the Expert window, refer to Chapter 4, "Expert Analyzer Capture and Display." Note that the Expert window is the same whether you are actively capturing frames, or engaged in post-capture display routines.

Getting More Information About a Diagnosis

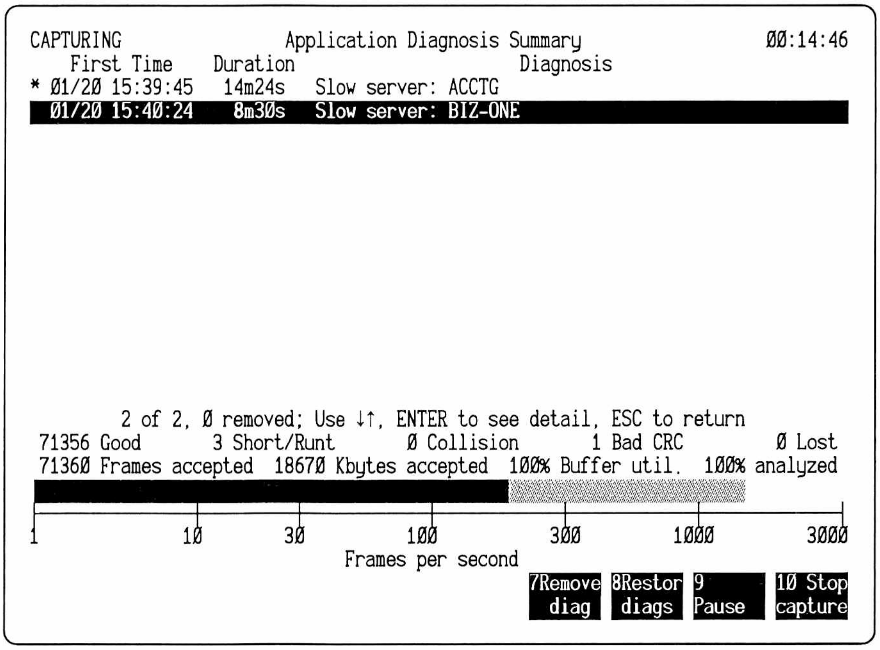
The Expert Overview shows the number of diagnoses per Expert layer but not the diagnoses themselves. You might want to view the list of diagnoses and elect to investigate one diagnosis at a time.

To obtain more information about a diagnosis:

1. In the Diagnoses column of the Expert Overview, use the cursor keys to highlight an Expert layer that exhibits at least one diagnosis. Press Enter.

   Result: A list of diagnoses at the selected Expert layer appears. Figure 2–6 is an example of the Diagnosis Summary screen at the Application layer.

   Note: If no diagnoses have been detected at the highlighted level, nothing will happen when you press Enter. If there are diagnoses at the highlighted layer, the help line at the bottom of the capture display will change to read, "`ENTER to see diagnoses.`"

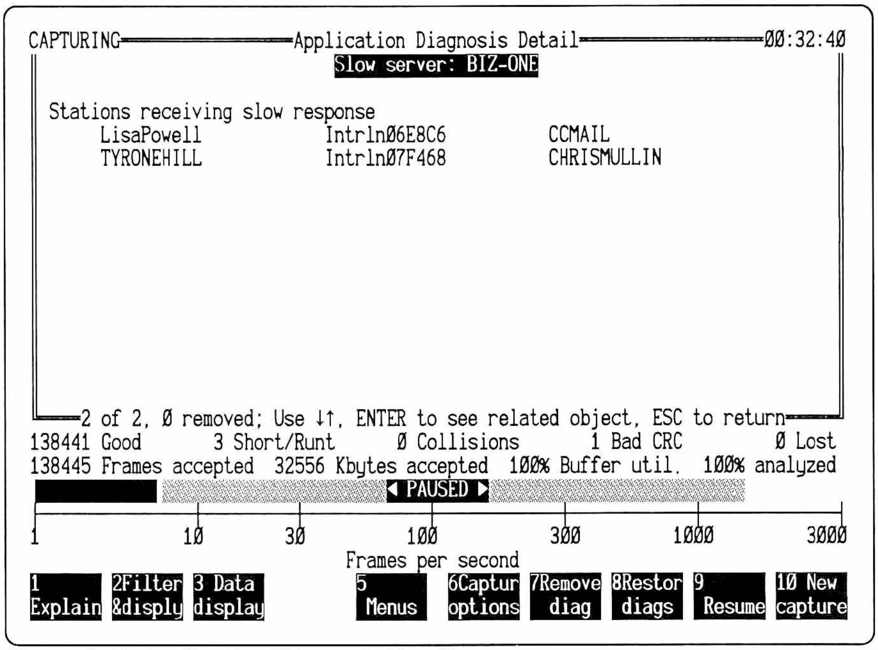


```
CAPTURING                Application Diagnosis Summary                    ØØ:14:46
    First Time    Duration                    Diagnosis
* Ø1/2Ø 15:39:45   14m24s   Slow server: ACCTG
  Ø1/2Ø 15:4Ø:24    8m3Øs   Slow server: BIZ-ONE









         2 of 2, Ø removed; Use ↓↑, ENTER to see detail, ESC to return
 71356 Good        3 Short/Runt       Ø Collision       1 Bad CRC          Ø Lost
 7136Ø Frames accepted  1867Ø Kbytes accepted  1ØØ% Buffer util.  1ØØ% analyzed

1               1Ø         3Ø          1ØØ          3ØØ          1ØØØ         3ØØØ
                                  Frames per second
```

Figure 2–6. Application Diagnosis Summary window. This view shows all diagnoses at the Application layer.

2. You can obtain more detailed information on any diagnosis. Use the cursor keys to highlight a diagnosis and press Enter to display a Diagnosis Detail screen, which contains further information regarding the selected diagnosis.

   For example, in Figure 2–6, the Diagnosis Summary view shows that the Expert analyzer has diagnosed the server BIZ-ONE as being slow. In Figure 2–7, the Diagnosis Detail screen shows which stations received a slow response from BIZ-ONE.



```
CAPTURING═══════════Application Diagnosis Detail══════════════ØØ:32:4Ø
                           Slow server: BIZ-ONE

 Stations receiving slow response
     LisaPowell           IntrlnØ6E8C6          CCMAIL
     TYRONEHILL           IntrlnØ7F468          CHRISMULLIN

═══2 of 2, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═══
138441 Good       3 Short/Runt      Ø Collisions      1 Bad CRC       Ø Lost
138445 Frames accepted  32556 Kbytes accepted  1ØØ% Buffer util.  1ØØ% analyzed
```

Figure 2–7. Application Diagnosis Detail screen.

The Diagnosis Detail screen in Figure 2–7 shows which nodes received a slow response from the server BIZ-ONE; however, it does not describe the network conditions that led the analyzer to arrive at this diagnosis or how you might go about correcting the problem. To get more information about this diagnosis, you may want to invoke the Expert analyzer's Explain screen.

Getting Context-Sensitive Explain Messages

The Expert analyzer displays concise diagnostic and symptom windows. If you do not fully understand the nature of the problem indicated by an Expert detail or summary window, or would like the opinion of the Expert analyzer, invoke the context-sensitive Explain message. Such a message tells you why the analyzer "thinks" that a problem exists, what other areas you might want to examine to determine the seriousness of the problem, and what thresholds affect the current symptom or diagnosis.

Explain messages are always available in the Expert window, whether during capture (if paused) or during post-capture display routines. You can pause capture at any time and invoke an Explain message. Do not confuse Explain messages with help messages, which are invoked by the same function key.

While viewing an Explain message, you can invoke Classic help "on top" of the Explain message. Help messages are also available anywhere in the analyzer's menus by pressing the F1 key.

The help messages serve as reminders about items in the analyzer's menus. Explain messages provide further information that is not in the current Expert view but may be important for your investigation of network problems. You can tell which type of message will appear by examining the dynamic function key labels at the bottom of the display. In Figure 2–7, F1 is labeled as **Explain**, and will display an Explain message when pressed, rather than a help message.

To display an Explain message during capture:

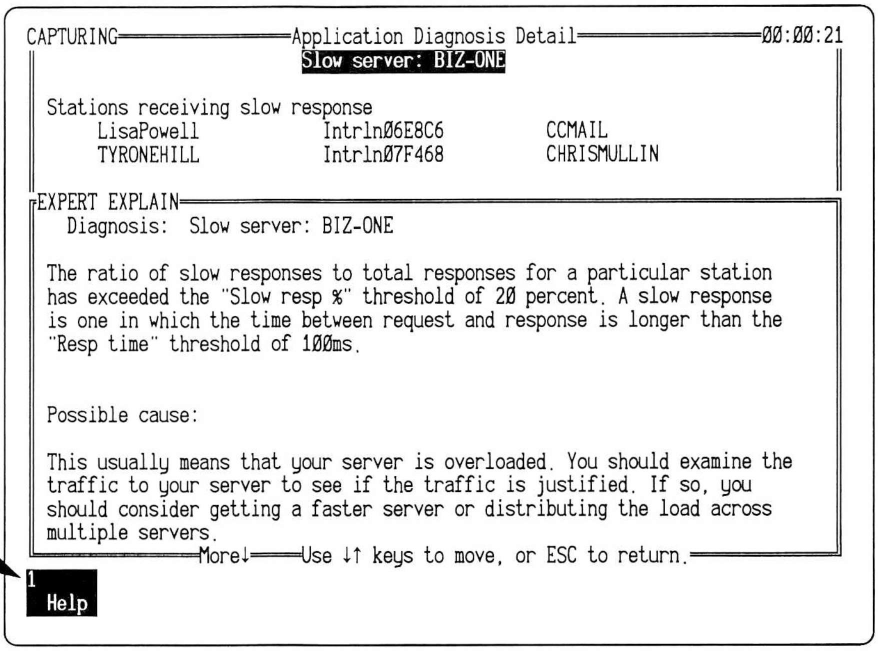
1. While in the Expert window, press F9 (**Pause**) to stop capture temporarily.
2. Press F1 (**Explain**).

   Result: The Expert analyzer displays a context-sensitive Explain message related to the current Expert view or highlighted item.

   Note: Classic help messages are available on top of Explain messages. The key label reading "Help" at the bottom of Figure 2–8 indicates this.

During post-capture display, Explain messages are always available in the Expert window by pressing F1.

Figure 2–8 shows the Explain message for the **Slow server** diagnosis from the previous example. Notice that the Application Diagnosis Detail view from Figure 2–7 is still visible behind the Explain screen.



```
CAPTURING══════════════Application Diagnosis Detail═════════════ØØ:ØØ:21
                               Slow server: BIZ-ONE

  Stations receiving slow response
       LisaPowell             Intrln06E8C6            CCMAIL
       TYRONEHILL             Intrln07F468            CHRISMULLIN

EXPERT EXPLAIN═══════════════════════════════════════════════════════
    Diagnosis:  Slow server: BIZ-ONE

  The ratio of slow responses to total responses for a particular station
  has exceeded the "Slow resp %" threshold of 2Ø percent. A slow response
  is one in which the time between request and response is longer than the
  "Resp time" threshold of 1ØØms.


  Possible cause:

  This usually means that your server is overloaded. You should examine the
  traffic to your server to see if the traffic is justified. If so, you
  should consider getting a faster server or distributing the load across
  multiple servers.
═══════════════More↓═════Use ↓↑ keys to move, or ESC to return.══════════
```

Notice that Classic help messages are available on top of Explain messages.

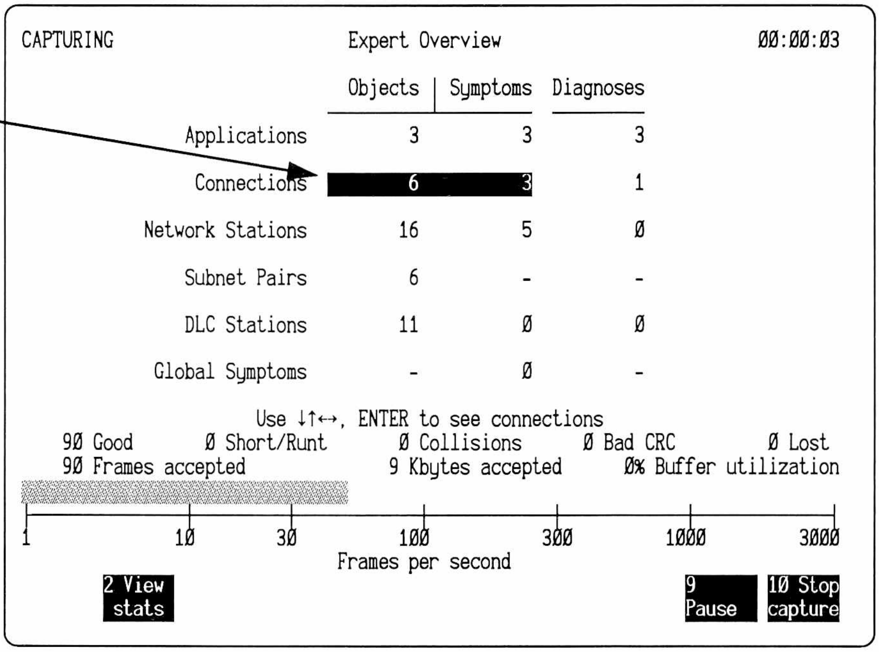
*Figure 2–8. Explain screen for the diagnosis, **Slow server**.*

Explain messages vary according to the context. For example, if the symptom message highlighted is "Many routers to remote network," the Explain message shows you specifically the connections among the network station and the routers. The network addresses and the configuration shown in the message can be different each time depending on the node and routers involved. Similarly, when you display a detail window for a diagnosis or symptom, the exact Explain message depends on the information in the detail window.

Getting More Information About Symptoms and Network Objects

You display the Expert analyzer's database of symptoms and network objects just as you would display information about diagnoses. From the Expert Overview, use the cursor keys to highlight the appropriate layer in the Objects/Symptoms column and press Enter. Figure 2–9 shows the Expert Overview with the Objects/Symptoms column highlighted at the Connections layer.

When you move the highlight to the Objects/Symptoms column, the highlight automatically expands to cover both columns. This indicates that you cannot view objects without viewing symptoms, and vice-versa.

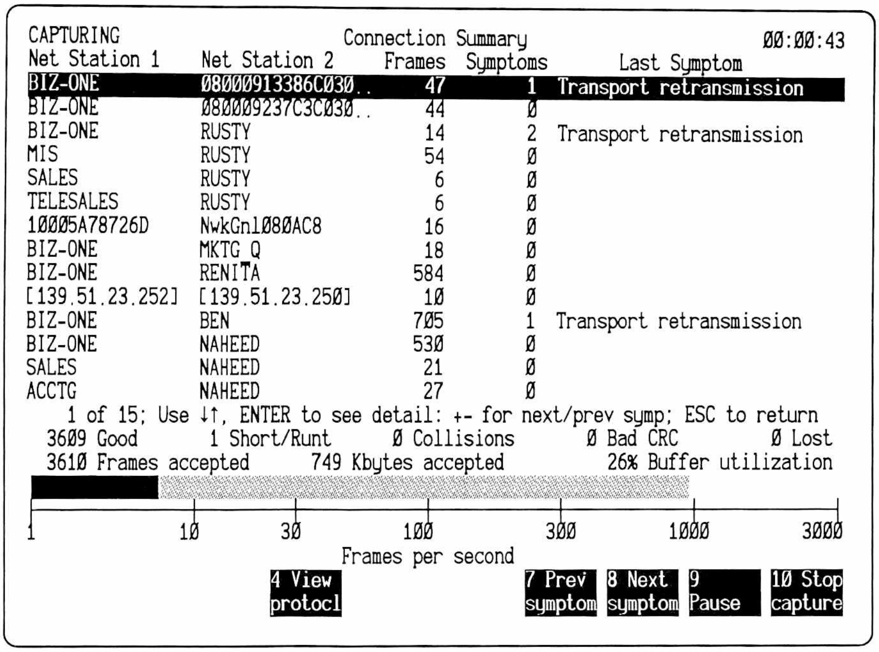


```
CAPTURING                        Expert Overview                      ØØ:ØØ:Ø3

                                Objects | Symptoms  Diagnoses

                  Applications        3         3          3
                   Connections        6         3          1
              Network Stations       16         5          Ø
                  Subnet Pairs        6         -          -
                  DLC Stations       11         Ø          Ø
              Global Symptoms         -         Ø          -

                        Use ↓↑↔, ENTER to see connections
  9Ø Good        Ø Short/Runt       Ø Collisions     Ø Bad CRC         Ø Lost
  9Ø Frames accepted               9 Kbytes accepted     Ø% Buffer utilization

1            1Ø       3Ø        1ØØ         3ØØ        1ØØØ        3ØØØ
                               Frames per second
```

You cannot view network objects without viewing symptoms.

Figure 2–9. Expert Overview with Objects/Symptoms column highlighted at Connections layer.

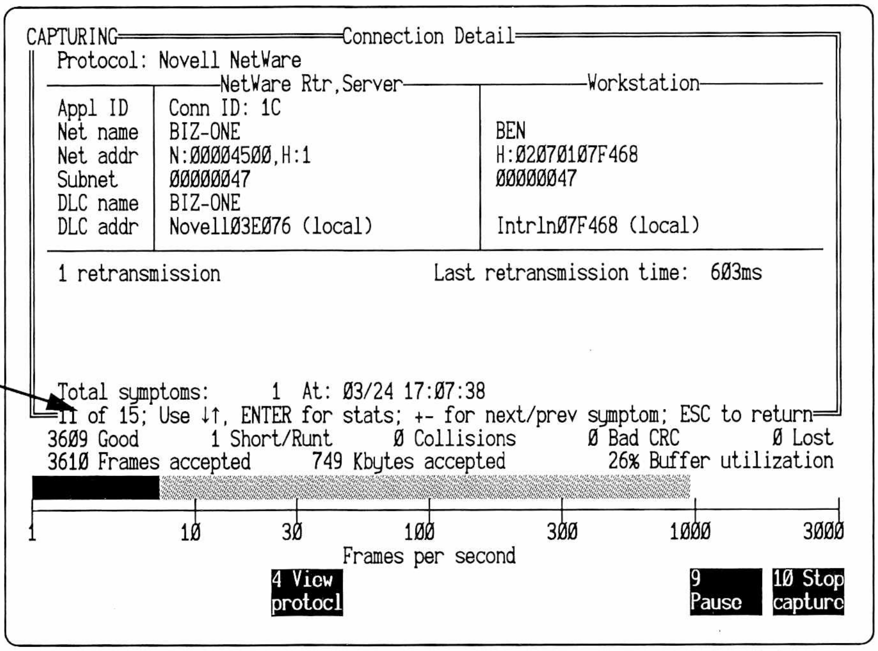
A list of network objects detected at the selected Expert layer appears. The list includes a description of the last symptom (if any) associated with each network object. This list is called a Summary window. Figure 2–10 is an example of the Summary window at the Connection layer.



```
CAPTURING                            Connection Summary                      ØØ:ØØ:43
Net Station 1    Net Station 2      Frames  Symptoms       Last Symptom
BIZ-ONE          Ø8ØØØ913386CØ3Ø..     47        1    Transport retransmission
BIZ-ONE          Ø8ØØØ9237C3CØ3Ø..     44        Ø
BIZ-ONE          RUSTY                 14        2    Transport retransmission
MIS              RUSTY                 54        Ø
SALES            RUSTY                  6        Ø
TELESALES        RUSTY                  6        Ø
1ØØØ5A78726D     NwkGn1Ø8ØAC8          16        Ø
BIZ-ONE          MKTG Q                18        Ø
BIZ-ONE          RENITA               584        Ø
[139.51.23.252]  [139.51.23.25Ø]       1Ø        Ø
BIZ-ONE          BEN                  7Ø5        1    Transport retransmission
BIZ-ONE          NAHEED               53Ø        Ø
SALES            NAHEED                21        Ø
ACCTG            NAHEED                27        Ø
     1 of 15; Use ↓↑, ENTER to see detail: +- for next/prev symp; ESC to return
   36Ø9 Good         1 Short/Runt        Ø Collisions         Ø Bad CRC        Ø Lost
   361Ø Frames accepted        749 Kbytes accepted          26% Buffer utilization
```

Figure 2–10. Connection Summary window.

To get detailed information about a particular connection or symptom, use the cursor keys to highlight a connection in the Summary window and press Enter. A detailed display appears as shown in Figure 2–11. The Detail window provides information such as the network addresses of the two endpoints of a connection, the protocol used, and any symptoms associated with the particular connection, network station, or DLC station.



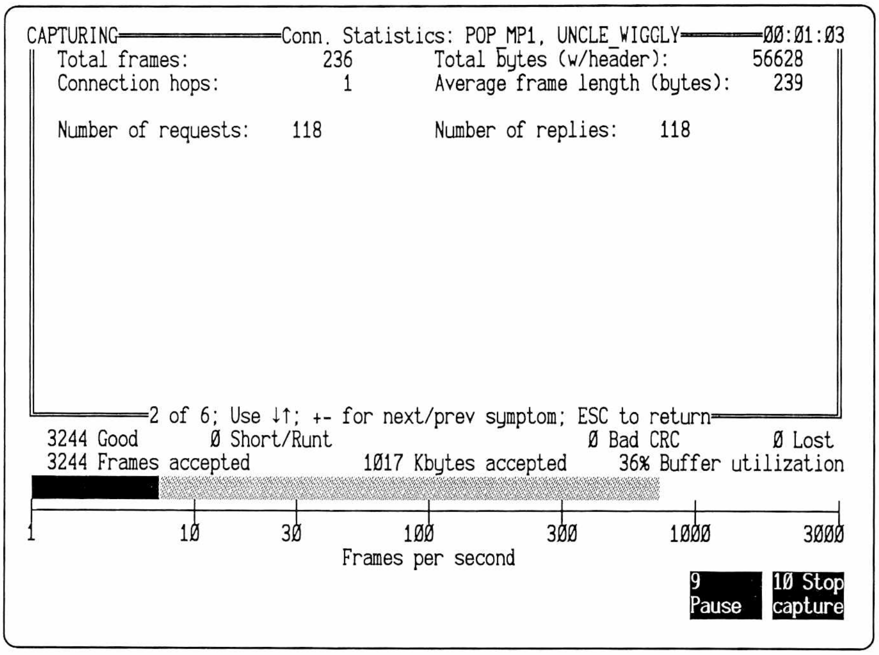
```
CAPTURING═════════════════════Connection Detail══════════════════════
 Protocol: Novell NetWare
 ─────────────NetWare Rtr,Server──────────────────────Workstation──────────
 Appl ID    Conn ID: 1C
 Net name   BIZ-ONE                         BEN
 Net addr   N:ØØØØ45ØØ,H:1                  H:Ø2Ø7Ø1Ø7F468
 Subnet     ØØØØØØ47                        ØØØØØØ47
 DLC name   BIZ-ONE
 DLC addr   NovellØ3EØ76 (local)            IntrlnØ7F468 (local)

 1 retransmission                     Last retransmission time:  6Ø3ms




 Total symptoms:       1  At: Ø3/24 17:Ø7:38
 1 of 15; Use ↓↑, ENTER for stats; +- for next/prev symptom; ESC to return
36Ø9 Good         1 Short/Runt        Ø Collisions         Ø Bad CRC        Ø Lost
361Ø Frames accepted        749 Kbytes accepted          26% Buffer utilization
```

You can use the cursor keys to scroll through the Detail windows for any of the 15 connections detected by the analyzer.

Figure 2–11. Connection Detail window. This window provides detailed information about a specific connection.

Notice that at the bottom of the Connection Detail border in Figure 2–11, the display reads, "11 of 15." From the Detail window, you can use the cursor keys to page through the Detail windows for any of the 15 connections detected by the Expert analyzer. Alternatively, you can press Enter again, and see a Statistics window for a particular connection, network station, or DLC station. Figure 2–12 shows a typical Statistics window at the Connection layer.

The exact information provided in the Statistics window depends both on the Expert layer at which it is displayed and the protocol involved. For example, at the Connections layer, the Statistics window shows the number of requests, number of replies, total bytes, and average frame length on a particular connection. The Statistics window at the Applications layer, however, includes statistics for application requests and average file transfer performance. In general, the Statistics window will quantify and describe network traffic to or from a highlighted station.



```
CAPTURING══════════════Conn. Statistics: POP_MP1, UNCLE_WIGGLY═══════ØØ:Ø1:Ø3
   Total frames:              236        Total bytes (w/header):        56628
   Connection hops:             1        Average frame length (bytes):    239

   Number of requests:    118            Number of replies:    118

════════════2 of 6; Use ↓↑; +- for next/prev symptom; ESC to return═════════
  3244 Good          Ø Short/Runt                        Ø Bad CRC          Ø Lost
  3244 Frames accepted          1Ø17 Kbytes accepted     36% Buffer utilization

1              1Ø        3Ø          1ØØ          3ØØ         1ØØØ         3ØØØ
                                Frames per second
```

Figure 2–12. Connection Statistics screen.

For more information on the various Expert displays available during capture, refer to Chapter 4, "Expert Analyzer Capture and Display."

Protocols Available for Expert Analysis

The Expert Sniffer analyzer can process frames on an Ethernet network segment a token ring, or a WAN link. The protocol suites that the Expert analyzer interprets as of the date of this manual include the following:

Protocol Family	Constituent Protocols
TCP/IP	IP, TCP, NFS, RPC, TELNET, FTP, ARP, SNMP, ICMP, RIP, EGP, SMB, UDP, GGP, IGRP, DNS, X-Windows
XNS	XNS, PEP, SPP, NCP, SMB
Novell	PEP, SPX, RIP, SAP, NetBIOS, NetWare
DECnet	DAP, NSP, DRP, LAT, SMB
WAN/Synchronous	Frame Relay, X.25, HDLC, IGRP (Cisco), Bridge/Router (various proprietary versions of HDLC)

Figure 2–13. Protocols currently available for Expert analysis.

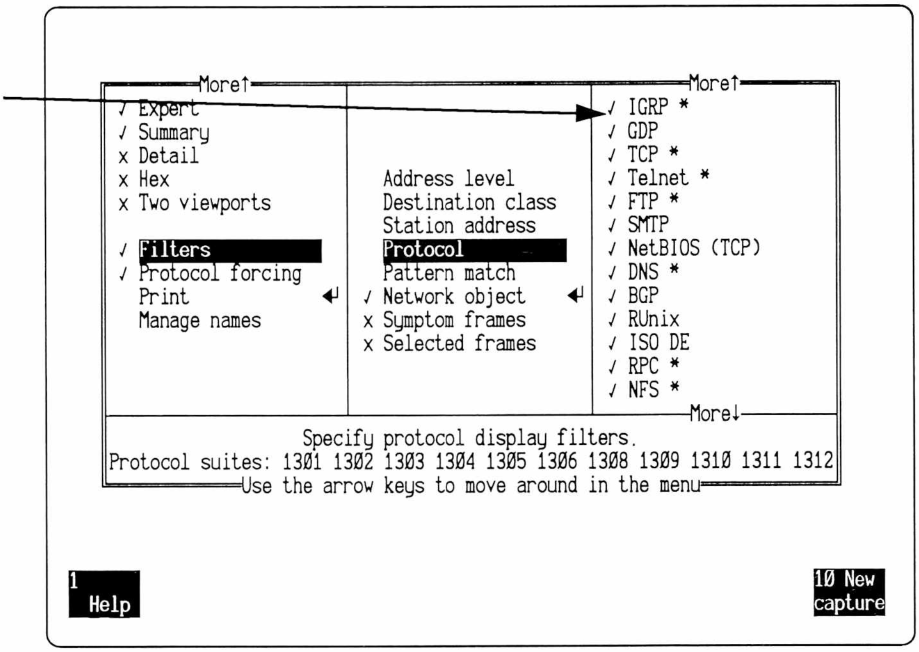
The Expert analyzer can perform Classic interpretation on many protocols for which Expert analysis is unavailable. The protocol suites on which your analyzer can perform Expert analysis may vary depending on the topologies installed. The procedure below shows you how to determine on which protocols your analyzer can perform Expert analysis.

To view the protocols on which your analyzer can perform Expert analysis:

1. Display the Main Menu of the Sniffer analyzer.
2. Use the cursor keys to move to the **Display\Filters\Protocol** menu.

   Result: The menu in Figure 2–14 appears.
3. Notice that some of the protocols listed in the right panel are followed by an asterisk. The analyzer can perform Expert analysis on those protocols followed by an asterisk.

The analyzer can perform Expert analysis on those protocols marked with an asterisk.



```
            More↑                                                    More↑
 √ Expert                                               √ IGRP *
 √ Summary                                              √ GDP
 x Detail                                               √ TCP *
 x Hex                    Address level                 √ Telnet *
 x Two viewports          Destination class             √ FTP *
                          Station address               √ SMTP
 √ Filters                Protocol                      √ NetBIOS (TCP)
 √ Protocol forcing       Pattern match                 √ DNS *
   Print            ↵   √ Network object          ↵     √ BGP
   Manage names         x Symptom frames                √ RUnix
                        x Selected frames               √ ISO DE
                                                        √ RPC *
                                                        √ NFS *
                                                         More↓
                         Specify protocol display filters.
Protocol suites: 13Ø1 13Ø2 13Ø3 13Ø4 13Ø5 13Ø6 13Ø8 13Ø9 131Ø 1311 1312
              Use the arrow keys to move around in the menu

1                                                                  1Ø New
 Help                                                              capture
```

Figure 2–14. The protocols on which the analyzer can perform Expert analysis.

DISTRIBUTED SNIFFER SYSTEM™

CHAPTER THREE: EXPERT ANALYZER OPTIONS 3

Network General

Expert Analyzer Options

Overview

This chapter explains the network layering scheme the Expert analyzer uses to categorize network problems and describes various precapture Expert options, including:

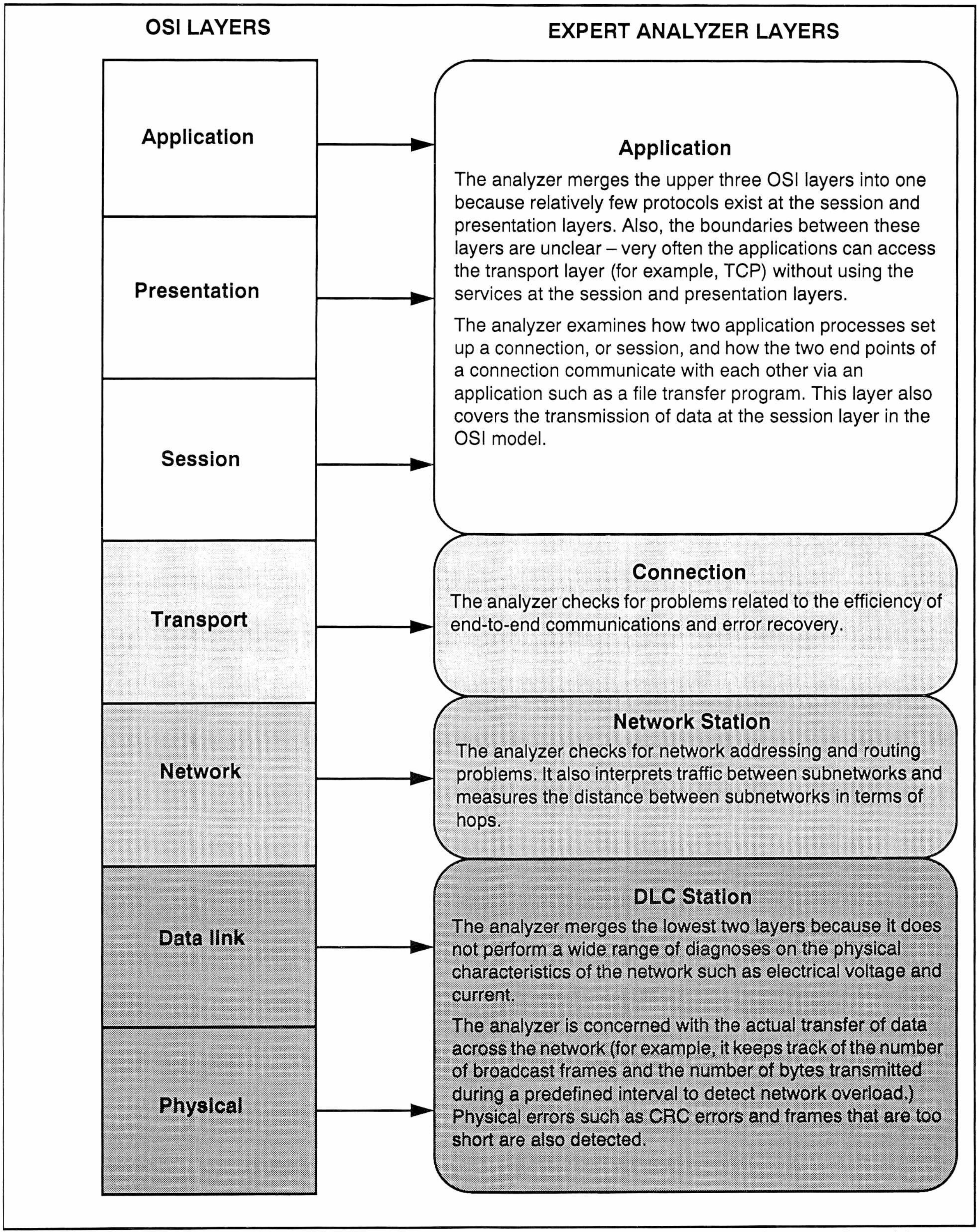
- How to specify TCP/IP subnet masks using the Expert analyzer's configuration function. You must be careful to configure the Expert analyzer with the subnet mask appropriate to the network it is analyzing. Configuring the Expert analyzer with an incorrect subnet mask can result in spurious symptoms and diagnoses in a TCP/IP environment.
- How to specify common Trustee names that should be excluded from the Expert analyzer's name search in a Novell environment.
- How to set Expert thresholds: You can adjust the Expert thresholds to control when the analyzer reveals symptoms and diagnoses.
- How to set alarm priorities to control the types of alarms sent to the Console.
- How to set a delay for reporting lower level alarms to the Console.
- How to set a delay on sending an alarm about the same diagnosis to the Console.
- How to set Expert triggers: Expert triggers allow you to specify a particular diagnosis as a trigger event, anchoring frames that interest you in the capture buffer.
- How to use the **Freeze/Reuse Allocation** and **Highest layer** options. These options help you to use memory and processor time optimally depending on your network analysis needs.

The chapter also describes how the analyzer learns the symbolic names of network entities by extracting relevant information from captured packets. When the analyzer learns a symbolic name, it will substitute that name for the address in the Expert displays. Several "tricks" to speed this process are discussed at the end of this chapter.

Expert Layers and the OSI Model

The Expert analyzer categorizes network problems according to the Expert layer at which they occur. During capture, the Expert analyzer uses its real-time protocol interpreters to map the information embedded in each frame onto its own model of network layers.

The network layering structure on the Expert analyzer is similar to the OSI model. However, the two schemes do not always exhibit a one-to-one mapping. Figure 3–1 explains what each Expert layer means and how it corresponds to the layers in the OSI model.



Application

The analyzer merges the upper three OSI layers into one because relatively few protocols exist at the session and presentation layers. Also, the boundaries between these layers are unclear – very often the applications can access the transport layer (for example, TCP) without using the services at the session and presentation layers.

The analyzer examines how two application processes set up a connection, or session, and how the two end points of a connection communicate with each other via an application such as a file transfer program. This layer also covers the transmission of data at the session layer in the OSI model.

Connection

The analyzer checks for problems related to the efficiency of end-to-end communications and error recovery.

Network Station

The analyzer checks for network addressing and routing problems. It also interprets traffic between subnetworks and measures the distance between subnetworks in terms of hops.

DLC Station

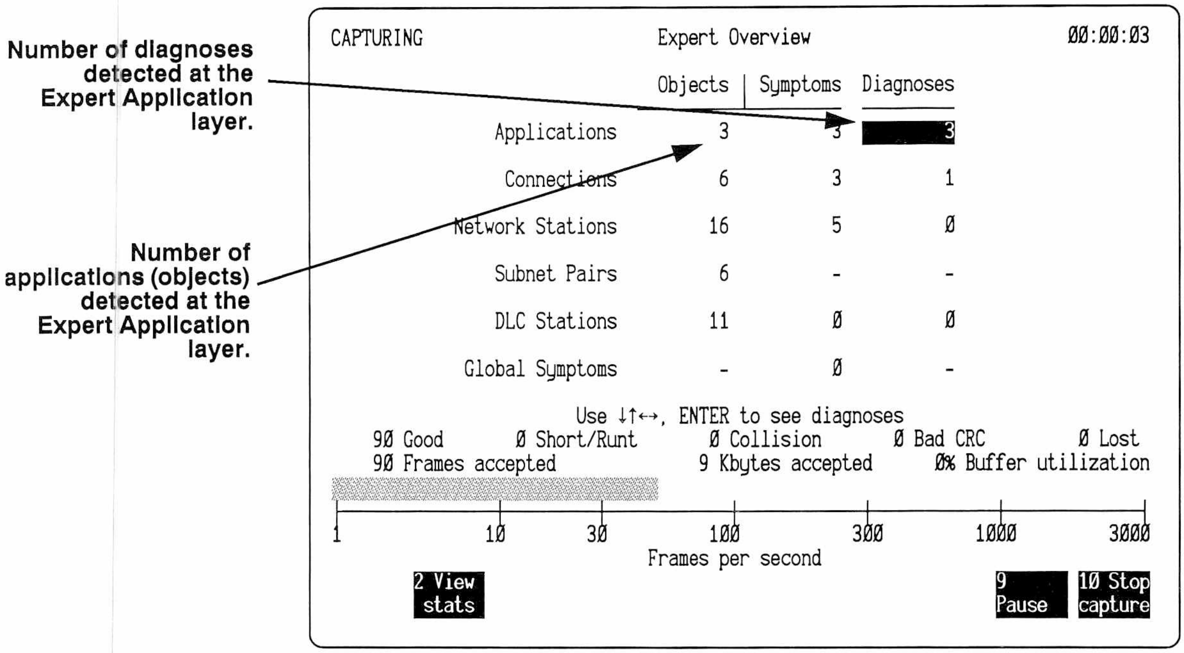
The analyzer merges the lowest two layers because it does not perform a wide range of diagnoses on the physical characteristics of the network such as electrical voltage and current.

The analyzer is concerned with the actual transfer of data across the network (for example, it keeps track of the number of broadcast frames and the number of bytes transmitted during a predefined interval to detect network overload.) Physical errors such as CRC errors and frames that are too short are also detected.

Figure 3–1. How the OSI model of network layers relates to the Expert's model.

The Expert analyzer's model of network layers is shown in the Expert Overview, illustrated in Figure 3–2. From this window, you can view subdisplays associated with network objects, symptoms, and diagnoses detected at the various Expert layers. For more information on the displays available in the Expert window, see Chapter 4, "Expert Analyzer Capture and Display."

Note: In addition to the four Expert layers, the Expert Overview also tallies Global Symptoms and Subnet Pairs. Global Symptoms are those symptoms which do not reside at any particular layer, such as Broadcast Storms. Subnet pairs provides information on all communicating subnets the Expert analyzer detects. These displays are described further in Chapter 4, "Expert Analyzer Capture and Display."



Number of diagnoses detected at the Expert Application layer.

Number of applications (objects) detected at the Expert Application layer.

```
CAPTURING                        Expert Overview                        ØØ:ØØ:Ø3

                                 Objects | Symptoms  Diagnoses

                   Applications        3         3          3
                    Connections        6         3          1
               Network Stations       16         5          Ø
                   Subnet Pairs        6         -          -
                   DLC Stations       11         Ø          Ø
                 Global Symptoms       -         Ø          -

                        Use ↓↑↔, ENTER to see diagnoses
   9Ø Good       Ø Short/Runt      Ø Collision      Ø Bad CRC       Ø Lost
   9Ø Frames accepted             9 Kbytes accepted    Ø% Buffer utilization

 1          1Ø     3Ø        1ØØ         3ØØ        1ØØØ        3ØØØ
                          Frames per second
```

Figure 3–2. The Diagnosis Overview window. The four Expert layers are displayed at left, along with Subnet Pairs and Global Symptoms.

The Expert layering structure is also used to group thresholds for symptoms and diagnoses in the **Expert settings** menu. For more information on Expert thresholds, see "Setting Thresholds for Symptoms and Diagnoses" on page 3–13.

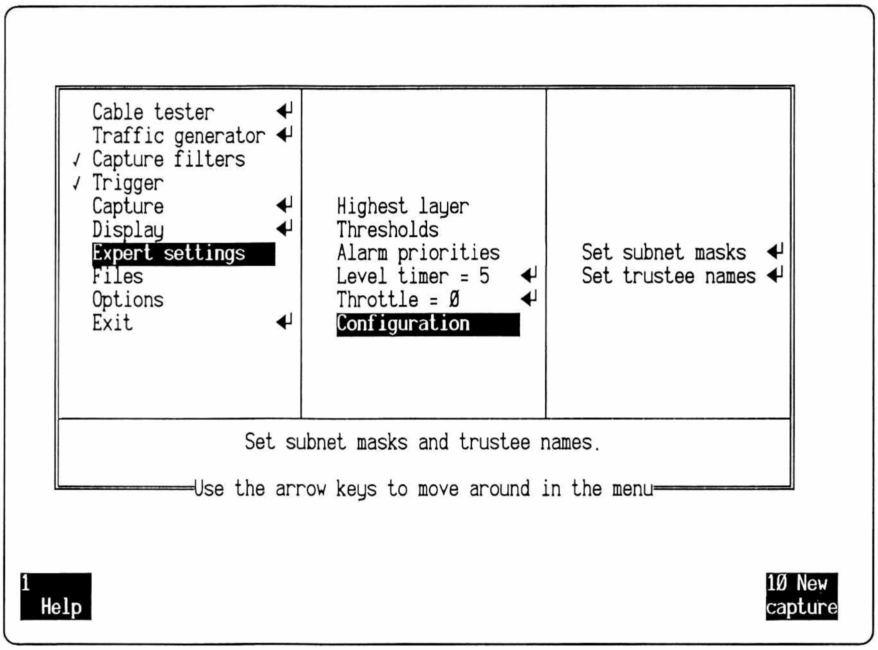
Configuring the Expert Analyzer

To ensure effective analysis of the network, two important options should be configured before capture begins. Whether or not you need to configure these options depends upon the protocol environment the Expert analyzer will observe.

• Subnet Masks	**Must** be configured for a TCP/IP environment.
• Trustee Names	Can be configured for a Novell environment.

To configure these items, use the Expert analyzer's configuration function, found in the **Expert settings\Configuration** menu. The changes made with the configuration function are saved to the appropriate STARTUP.xxV file (where xx=EN for Ethernet, TR for token ring, or SY for WAN/Synchronous). For more information on the analyzer's use of files, see the *Distributed Sniffer System: Analyzer Operations Manual.*

Figure 3–3 shows the Expert analyzer's **Expert settings\Configuration** menu.



Set subnet masks and trustee names.

Use the arrow keys to move around in the menu

Figure 3–3. Configuration menu of the Expert Sniffer analyzer.

Setting Subnet Masks

A traditional standard of TCP/IP subnet masks exists, which reserves specific bits within an IP network address for the subnet mask, depending on the class of address. The Expert analyzer comes with default subnet mask settings for each class of IP address:

IP ADDRESS	EXPERT DEFAULT SUBNET MASK
Class A	[255.255.0.0]

Class B	[255.255.255.0]
Class C	[255.255.255.0]

Networks may use non-traditional subnet masks. If the Expert analyzer is attached to a network segment which uses non-traditional subnet masks, it is possible that the analyzer will register spurious network objects and diagnoses. This happens because the analyzer expects address information at a location within the address field other than where it actually is.

Example: Using an Incorrect Subnet Mask

Figure 3–4 shows two different legal Class A IP broadcast addresses.

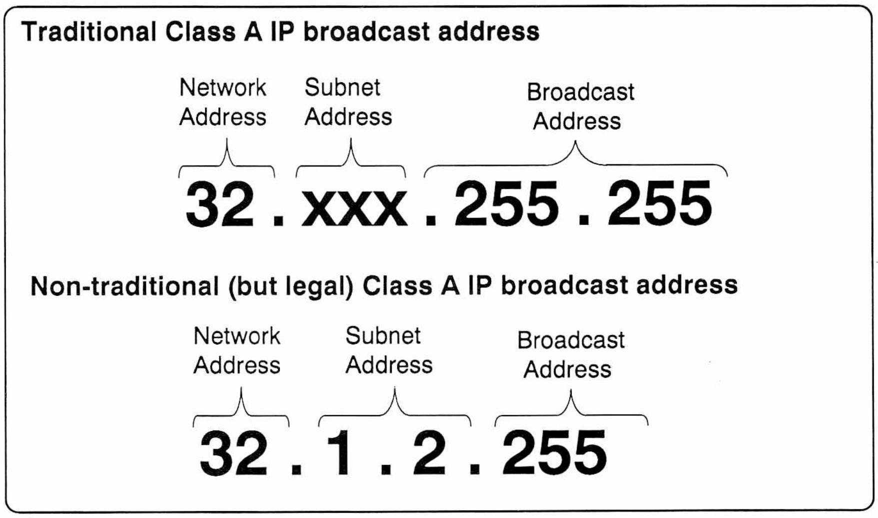


Figure 3–4. Two different Class A IP broadcast addresses.

The first address represents a traditional Class A IP broadcast address. The first field of the address is the network address, the second field is the subnet address, and the last two fields are the host address (in this case, broadcast). The Expert analyzer will correctly analyze this frame, using its default Class A subnet mask.

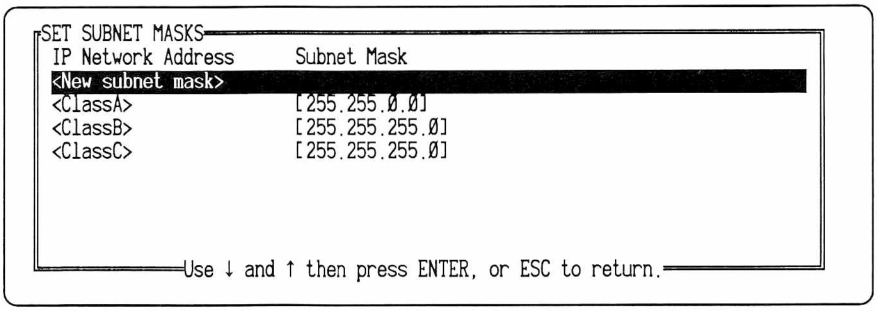
The second address shows a non-traditional Class A IP broadcast address. Instead of limiting the subnet address to the second field, this address uses the second and third fields as the subnet address, and only the fourth field as the host address (still broadcast). Using the default Class A subnet mask, the Expert analyzer would mistakenly interpret the subnet address as 1. The Expert analyzer would fail to register the broadcast address, and would create a spurious network object for the host address 2.255.

It is essential that you enter the IP network address and appropriate subnet mask for the networks from which the Expert analyzer will see frames. Failure to do so can result in false network objects and diagnoses.

The Expert analyzer's configuration function allows you to add, delete, or change user-configured subnet masks. You can also edit or delete the analyzer's default subnet masks.

To add a specific IP network address and associated subnet mask:

1. Move to the **Expert settings\Configuration\Set subnet masks** option.
2. Press Enter. The box in Figure 3–5 appears.



```
SET SUBNET MASKS
 IP Network Address         Subnet Mask
<New subnet mask>
<ClassA>                    [255.255.Ø.Ø]
<ClassB>                    [255.255.255.Ø]
<ClassC>                    [255.255.255.Ø]

          Use ↓ and ↑ then press ENTER, or ESC to return.
```

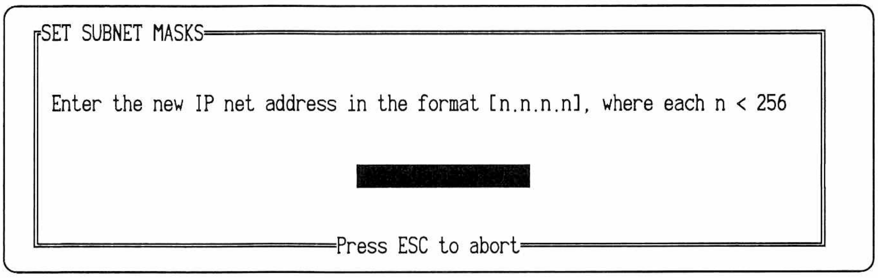
Figure 3–5. Set Subnet Masks box.

3. Highlight `<New subnet mask>`, and press Enter.

   Note: If you have already entered the maximum number of addresses, the analyzer will indicate this. You will need to delete one of the existing addresses first. See the next procedure, on page 3–10.

4. The box in Figure 3–6 appears. Type in the new IP network address in the format [n.n.n.n], where each n is less than 256, and press Enter.

   Note: The brackets are optional. However, if you include one bracket, you must include both.

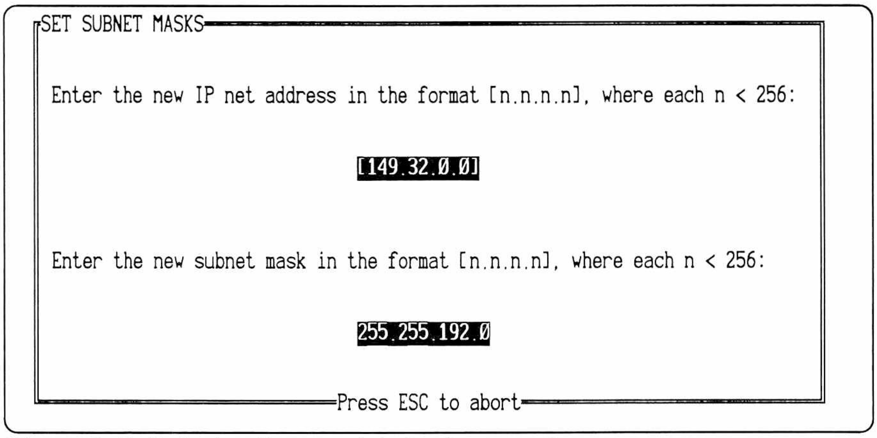


```
SET SUBNET MASKS

Enter the new IP net address in the format [n.n.n.n], where each n < 256



                         Press ESC to abort
```

Figure 3–6. Entering the IP network address.

5. After you press Enter, a box (Figure 3–7) appears in which you enter the subnet mask associated with the IP network address you just entered. Enter the subnet mask in the form [n.n.n.n], and press Enter.

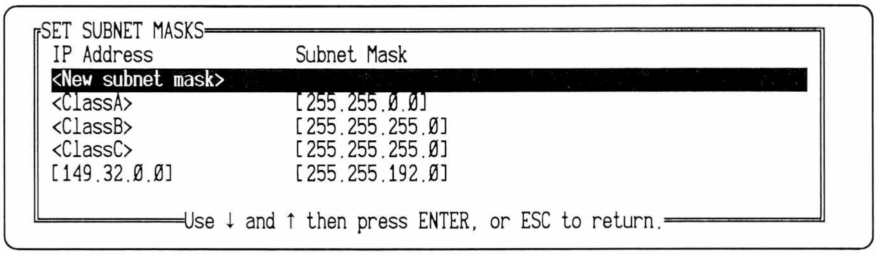
   Note: Depending on the class IP network address you entered, the analyzer may supply the first fields of the subnet mask for you. The analyzer will not allow you to enter an illegal network address/subnet mask pair.



```
SET SUBNET MASKS

 Enter the new IP net address in the format [n.n.n.n], where each n < 256:

                              [149.32.0.0]

 Enter the new subnet mask in the format [n.n.n.n], where each n < 256:

                              255.255.192.0

                         Press ESC to abort
```

Figure 3–7. Entering the associated subnet mask.

6. After you have entered the IP network address and subnet mask, the analyzer adds the new entries to the list in Figure 3–8.



```
SET SUBNET MASKS
 IP Address             Subnet Mask
 <New subnet mask>
 <ClassA>               [255.255.0.0]
 <ClassB>               [255.255.255.0]
 <ClassC>               [255.255.255.0]
 [149.32.0.0]           [255.255.192.0]

          Use ↓ and ↑ then press ENTER, or ESC to return.
```

Figure 3–8. List of defined IP network addresses and subnet masks.

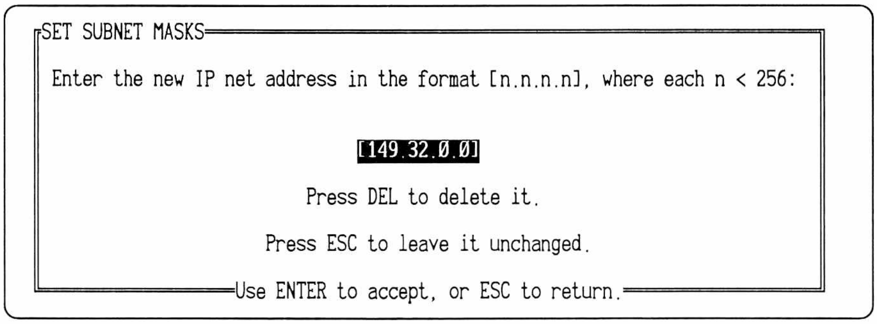
You can also modify or delete existing IP network addresses and subnet masks.

To modify or delete existing IP network addresses and subnet masks:

1. Move to the **Expert settings\Configuration\Set subnet masks** option and press Enter. The list in Figure 3–5 appears.

2. Highlight the IP network address and associated subnet mask you want to modify or delete and press Enter.

   The box in Figure 3–9 appears.



```
SET SUBNET MASKS
 Enter the new IP net address in the format [n.n.n.n], where each n < 256:

                              [149.32.0.0]

                          Press DEL to delete it.

                       Press ESC to leave it unchanged.

               Use ENTER to accept, or ESC to return.
```

Figure 3–9. Modifying or deleting the IP address.

3. Do you want to delete this IP network address?

— If so, press the Delete key. The analyzer posts a warning box and then deletes both the IP address and the associated subnet mask.

— If not, either press ESC to return to the Set Subnet Mask box, or modify the IP network address and subnet mask using the cursor keys.

4. Once you have deleted or modified the IP network address and subnet mask pair, the analyzer updates the list in Figure 3–8.

As the Expert analyzer captures TCP/IP frames, it will first check its list of user-configured IP network addresses and subnet masks and try to associate the proper address with the incoming frames. If the analyzer does not find the appropriate address in its list of addresses, it will apply the default subnet mask appropriate to the class of address it is currently analyzing.

Changes made by the Expert analyzer configuration function become active immediately. There is no need to restart the application. Additionally, any changes made by the Expert analyzer configuration function are automatically saved to the STARTUP.xxV file when you exit the analyzer. The next time the analyzer starts, it will start with the changes you made intact.

Setting Trustee Names

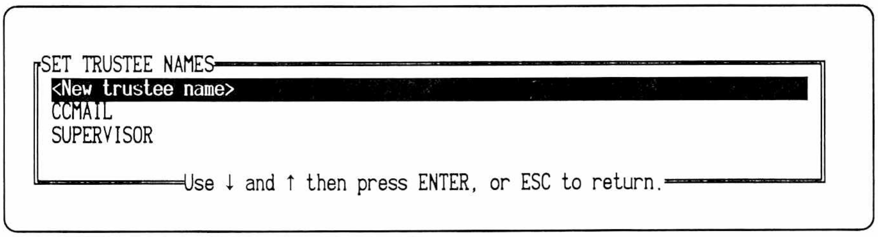
One of the central functions of the Expert analyzer is its ability to learn symbolic names by extracting information from the packets that pass through its real-time protocol interpreters. The Expert analyzer does this automatically, substituting symbolic names for addresses in the Expert displays as it learns them.

Because the Novell environment often uses trustee names to refer to groups of users during bindery requests, the analyzer may incorrectly substitute a name for a network address. For example, suppose the user Agnes is a member of the trustee group CCMAIL. When Agnes requests access to her CCMAIL, the Novell software will first check the bindery for the trustee name CCMAIL and then check if Agnes is a valid member of this group. During the course of this transaction, the analyzer may associate the trustee name CCMAIL with Agnes' station address.

To prevent inaccurate name-address assignment from happening, you can use the Expert analyzer's configuration function to specify trustee names that will be excluded from the Novell name search.

To specify trustee names to be excluded from the Novell name search:

1. Move to the **Expert settings\Configuration\Set trustee names** menu option.
2. Press Enter. The box in Figure 3–10 appears.

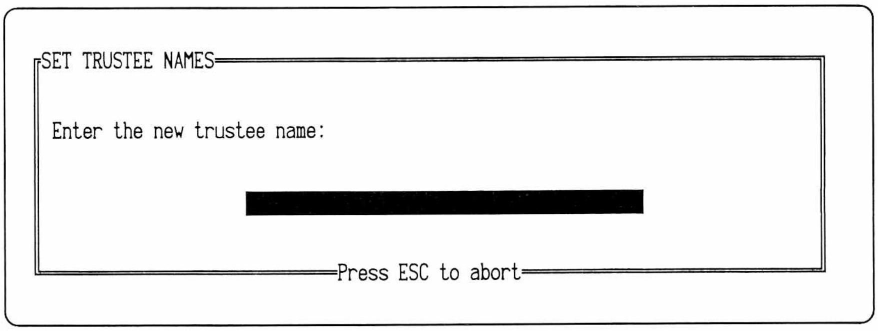


```
SET TRUSTEE NAMES
<New trustee name>
CCMAIL
SUPERVISOR

Use ↓ and ↑ then press ENTER, or ESC to return.
```

Figure 3–10. Set Trustee Names box

3. Highlight `<New trustee name>` and press Enter. The box in Figure 3–11 appears.

   Note: If the maximum number of trustee names has already been entered, a pop-up box will inform you of this. You will need to delete an existing trustee name in order to add a new one.



```
SET TRUSTEE NAMES

Enter the new trustee name:



Press ESC to abort
```

Figure 3–11. Entering a new Trustee Name.

4. Enter the trustee name which you want the Expert analyzer to ignore during the Novell name search. The following common names are provided by default:
   - CCMAIL
   - SUPERVISOR
5. Press Enter. After the name has been entered, it will appear in the Set Trustee Names box in Figure 3–10.

To delete or modify trustee names:

1. Use the procedure above to go to the Set Trustee Names box.
2. In the list that appears, highlight the name you want to modify or delete. Press Enter.
3. In the box that appears, you can press the Delete key to delete a trustee name or modify a name using the keyboard.

Changes made by the Expert analyzer configuration function become active immediately. There is no need to restart the application. Additionally, any changes made by the Expert analyzer configuration function are automatically saved to the STARTUP.xxV file when you exit the analyzer. The next time the analyzer starts, it will start with the changes you made intact.

Setting Thresholds for Symptoms and Diagnoses

The thresholds in the analyzer's **Expert settings\Thresholds** menu determine whether the analyzer generates a symptom or diagnosis message based on a given network event. This section describes how to set the Expert thresholds.

The default thresholds supplied with the Expert analyzer have been carefully calculated to ensure accurate and informative symptom and diagnosis detection. Before changing any of the thresholds, make sure you understand:

- How the Expert thresholds interact with one another to determine symptom and diagnosis detection. This section describes each threshold, and the symptoms and diagnoses associated with them.
- Your network. The final responsibility for creating an informative set of Expert thresholds lies with you. You should not change any of the Expert thresholds until you have established a network baseline and are sure the new values are appropriate for your particular network.

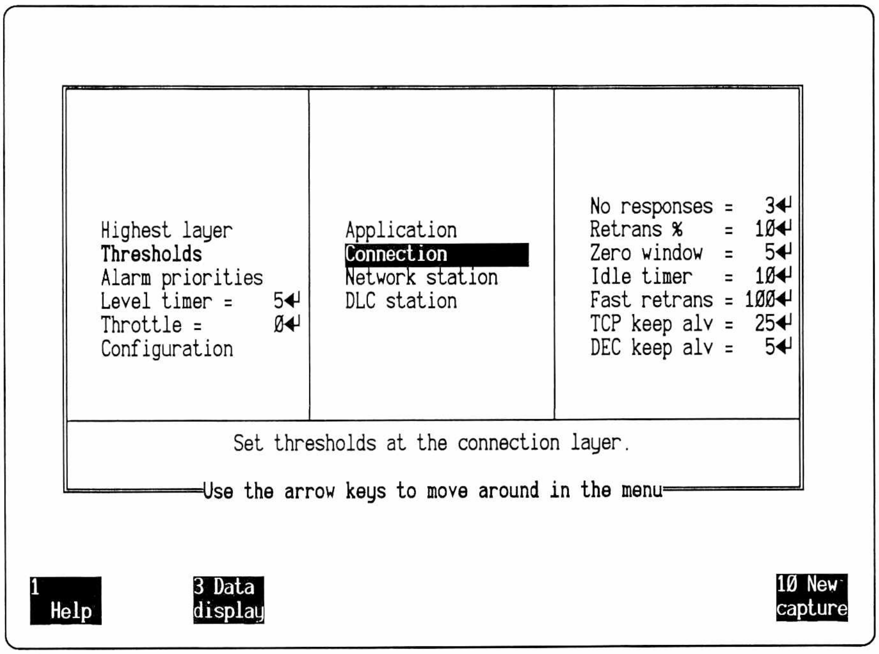
  For example, after capturing with the default Expert thresholds you may find that the analyzer is registering repeated **LAN overload** diagnoses. Upon closer examination you find that the amount of traffic on this particular segment was, in fact, quite normal for your particular network. If that is the case, you may want to increase the **LAN overload** threshold to a higher rate of traffic, ensuring that the analyzer reveals a diagnosis only when the amount of traffic on this segment presents a problem.

Note: You can always use the **Use defaults** command in the Options menu to reset all the Expert thresholds to their original values. Be aware that the **Use defaults** command will reset all settings in the analyzer's menus to their original values. For more information on using the **Use defaults** command, refer to the *Sniffer Network Analyzer Operations* manual.

To set an Expert threshold:

1. From the Main Menu, use the cursor keys to move to the **Expert settings\Thresholds** menu.
2. Move the highlight to the Expert layer associated with the threshold you want to change.

   Result: The right panel displays a list of thresholds associated with the highlighted layer, as shown for the Connection layer in Figure 3–12.



```
                                                         No responses =   3↵
Highest layer            Application                     Retrans %    =  10↵
Thresholds               Connection                      Zero window  =   5↵
Alarm priorities         Network station                 Idle timer   =  10↵
Level timer =      5↵    DLC station                     Fast retrans = 100↵
Throttle =         0↵                                    TCP keep alv =  25↵
Configuration                                            DEC keep alv =   5↵

                      Set thresholds at the connection layer.

               Use the arrow keys to move around in the menu

1 Help          3 Data display                                    10 New capture
```

Figure 3–12. The Expert settings \ Thresholds \ Connection layer menu.

3. Use the cursor keys to move the highlight to the desired threshold. Press Enter.

   Result: A dialog box opens.

4. Type the new value for the desired threshold and press Enter.

The newly defined threshold takes effect the next time you do either of the following:

- Start capture in Expert mode
- Display the frames in the capture buffer

When you display frames after changing an Expert threshold, the analyzer automatically performs Expert analysis on all frames in the capture buffer, generating symptom and diagnosis messages according to the new Expert thresholds. Previous analysis results are lost. For more information on this concept, see "Effects of Changing Expert Thresholds" on page 3–30.

Symptom and Diagnosis Thresholds at Each Expert Layer

This section describes the meaning of each user-defined Expert threshold and how it affects symptom and diagnosis detection. Depending on the topologies you ordered from the factory, the exact thresholds available on your analyzer may be a subset of those described here. Figure 3–13 shows the available thresholds at each Expert layer. The thresholds are described in the same order in which they appear in the analyzer's menus.

How the Expert Thresholds Interact

Many of the Expert thresholds work in tandem to determine symptom and diagnosis detection. For example, at the Data Link layer, the analyzer displays a symptom message when network traffic exceeds the Expert threshold, **LAN overload** (by default, 30 percent of available bandwidth). In each minute, if network traffic exceeds the **LAN overload** threshold for more than 20 percent of the time (defined by the threshold **LAN overload %**), the analyzer will diagnose that the network is overloaded.

In other words, one threshold (**LAN overload**) specifies when a symptom is detected. The second threshold, usually specified as a percentage (in this case, **LAN overload %**), specifies at what point a symptom becomes problematic enough to be considered a diagnosis. Figure 3–13 indicates pairs of thresholds that work in this manner by displaying them side by side.

Expert Layer	Expert Threshold	Related Expert Threshold
Application Layer	Minimum Application Requests	
	Response Time	Slow Response Percentage
	Filter Time	Denied Count
	Filter Time	Loop Percentage
	Denied Request Percentage	
	Local Transfer/Remote Transfer	Slow File Percentage
Connection Layer	No Responses	
	Retransmission Percentage	
	Zero Window	
	Idle Timer	
	Fast Retransmission	
	TCP Keep Alive	
	DEC Keep Alive	
Network Layer	Multiple Routers	
	DEC Hello	
	Duplicate Percentage	
DLC Station Layer	LAN Overload	LAN Overload Percentage
	Broadcast Symptom	Broadcast Diagnosis
	Physical Errors	
	WAN Overload*	WAN Overload Timer*
	WAN Underload*	WAN Underload Timer*
	Congestion Percentage*	
MAC Layer (Token Ring)	Ring Entries	
	Receiver Congestion	
	Station Removed	
	Ring Errors	
	Ring Purge Symptom	Ring Purge Diagnosis

* WAN/Synchronous (Sniffer Internetwork Analyzer) only.

Figure 3–13. Expert thresholds available at each Expert layer.

Application Thresholds

The Expert thresholds at the Expert Application layer are related to the quality of connections and file transfers. The thresholds are described in the same order as they appear in Figure 3–13.

Minimum Application Requests

The **Min appl req** threshold specifies the minimum number of application requests that must have been sent by a specific application before the analyzer will display an Application layer diagnosis related to that application.

Suppose **Min appl req** is set to 100 (the default). If Station A has sent Station B 25 file requests and a file retransmission occurs, the analyzer will not generate the **File retransmission** diagnosis (or any other diagnosis) because there have not yet been 100 application requests between Station A and Station B. The **Min appl req** threshold helps ensure that the Expert analyzer bases a symptom or diagnosis on reliable statistics, not a few isolated instances of abnormal network activities at the Application layer.

Possible values range from 0 to 999; default value is 100.

Response Time

The threshold **Response time** specifies the time limit within which a Server should respond to an application request. If the Server sends a response after the timer expires, the analyzer considers the response "slow." This threshold alone does not generate a symptom or diagnosis. However, if the ratio of slow responses to normal responses exceeds the threshold set by **Slow resp %**, the analyzer generates the diagnosis **Slow server**.

Response time measures the time (in milliseconds) between when an application request is sent and a response is received.

Possible values range from 0 to 999 milliseconds; default value is 100 milliseconds.

Slow Response Percentage

The **Slow Response Percentage** threshold determines whether the analyzer considers a server slow in responding to application requests. The diagnosis is **Slow server**.

The value is the ratio between slow responses and normal responses in percentage. This percentage is calculated by the following expression:

Number of slow responses / Number of normal responses x 100

A response is considered slow if the response time exceeds the value defined by the threshold **Response time**.

Possible values for the **Response time %** threshold range from 0 to 100 percent; default value is 20 percent.

Filter Time

The **Filter time** threshold specifies (in seconds) the maximum time interval during which the analyzer counts repeated requests and denied requests. Each time an application process sends out a request, the analyzer resets the filter timer. If the same request is sent out again before the filter timer expires, the second request is considered a repeated request. For example, if the **Filter time** threshold is set to five seconds and an application sends out the same request one minute after the first one, the second request is not considered a repeated request.

The **Filter time** threshold also determines whether the analyzer counts a given denied request. For example, some printers poll servers at regular intervals (such as once every five seconds) to find out if there are print jobs in their queues. If there are no print jobs, the printer's request is denied. Because this is a regular occurrence, you should set **Filter time** low enough so that the analyzer will not register normal network activity (a server denying a printer's request) as excessive denied requests. In this example, if **Filter time** were set less than five seconds, the repeated server polls by the printer would not be counted as denied requests.

The **Filter time** threshold by itself does not result in a diagnosis. However, in tandem with the **Loop %** threshold (see below), it does affect when the diagnosis, "Too many loops (*number of loops*) by *station name* to *station name*," appears.

Additionally, in tandem with the **Denied count** and the **Denied request percentage** threshold, the **Filter time** threshold controls when the symptom, "*x* denied requests," and the diagnosis, "Excessive denied requests," appear.

Possible values for the **Filter time** threshold range from 0 to 999 seconds; default is 1 second.

Denied Count

The **Denied count** threshold specifies the quantity of denied requests for a given application at which the analyzer will generate the symptom "*x* denied requests." Notice that the analyzer defines denied requests using the **Filter time** threshold. That is, a request is only counted as denied if it is denied within the time range specified by the **Filter time** threshold (see above for details).

For example, suppose the following thresholds were set:

- **Filter time** = 1 second
- **Denied count** = 2

In this case, the analyzer will only count a request as denied if it occurs within one second from the last denied request. Once the analyzer detects more than two denied requests for a given application, it generates the "*x* denied requests" symptom.

Possible values for the Denied count threshold range from 1 to 100. The default is 2.

Loop Percentage

While the threshold **Filter time** specifies at what point the analyzer considers an application process request to be a repeated request, the threshold **Loop %** specifies at what point the quantity of these repeated requests presents a problem.

The value of **Loop %** is the ratio between repeated requests and normal requests. A repeated request is one that is sent out even though the proper response to the previous request has already been seen by the analyzer. The analyzer does not count certain repeated requests. For example, if a repeated request is sent after the **Filter time** threshold expires, the analyzer "forgets" the previous request and does not consider this one a repeated request. A normal request is any request that is not deemed repeated by the analyzer.

Note: Repeated requests exclude the read or write requests involved in file transfers.

The analyzer calculates the value for **Loop %** by the following equation:

Number of Repeated Requests / Number of Normal Requests *x* 100

The diagnosis is, "Too many loops (*number of loops*) by *station name* to *station name*." The analyzer displays separate diagnosis messages for different connections, even if the connections originate from the same station. For example, if Station A is sending a high number of repeated requests to both Server 1 and Server 2, the following diagnoses appear:

Too many loops (68) by Station A to Server 1
Too many loops (70) by Station A to Server 2

Possible values for the **Loop %** threshold range from 0 to 100 percent; default value is 30 percent.

Denied Request Percentage

The **Denied req %** threshold specifies the maximum acceptable percentage of denied versus successful application requests for a given application. If this percentage is exceeded, the analyzer reveals the diagnosis, **Excessive requests denied from *station name*.**

The value for **Denied req %** is calculated as follows:

Number of denied requests / Number of successful requests *x* 100

Note that the analyzer uses the **Filter time** threshold to determine whether it should consider a request as denied or not. See the **Filter time** section on page 3–18.

Possible values range from 0 to 100 percent; the default is 20 percent.

Local Transfer/ Remote Transfer

The **Local Transfer** and **Remote Transfer** thresholds specify the minimum acceptable rate of data transfer for a file transfer between two stations. If the rate of a given file transfer falls below the specified minimum data rate, the analyzer will reveal the symptom **Low Throughput**.

Meaning:

- **Local transfer**– Speed of file transfer between two stations on the same subnetwork. Possible values range from 0 to 999 Kbytes/s; default is 200 Kbytes/s.
- **Remote transfer**– Speed of file transfer between two stations separated by at least one bridge/router (that is, with a hop count greater than or equal to one). Possible values range from 0 to 999 Kbytes/s; default is 50 Kbytes/s.

Note: Local transfer and **Remote transfer** are separate thresholds. The analyzer applies two different minimum transfer rates depending on whether a given connection is defined as remote or local. Local transfers have hop counts of zero. Remote transfers have hop counts of one or more. Normally, file transfer becomes slower as the hop count increases, so you should set the **Local transfer** threshold to a greater value than **Remote transfer**.

The frequency of slow file transfers between two stations affects when the analyzer displays the diagnosis, **Slow File Transfer**. See the definition for **Slow File Percentage**, below.

Slow File Percentage

The **Slow File Percentage** threshold specifies the maximum percentage of slow file transfers versus normal file transfers for a given connection. If the specified ratio is exceeded, the analyzer diagnoses that the file transfer process between two stations is too slow. The diagnosis is **Slow File Transfer**.

Slow File Percentage is calculated as the ratio between slow file transfers and normal file transfers. Slow file transfers are those whose rates are less than the **Local transfer** or **Remote transfer** thresholds. Normal file transfers are those whose rate exceeds the minimum acceptable data rate specified by the **Local transfer** or **Remote transfer** thresholds. **Slow File Percentage** is calculated by the following equation:

Number of slow file transfers / Number of normal file transfers x 100

Note: The analyzer will make a diagnosis only after 10 file transfers have taken place.

Possible values range from 0 to 100 percent; default value is 30 percent.

File Overlap/Retransmissions

Note: The **Slow file percentage** threshold also specifies the maximum percentage of file retransmissions versus normal file transfers for a given connection. If the specified ratio is exceeded, the analyzer diagnoses that there are too many retransmissions on the connection. The diagnosis is **File overlap/retransmissions**.

Connection Thresholds

The Expert thresholds in this section refer to specific connections detected at the Expert Connection layer. The thresholds are organized in the same order they are found in the **Expert settings\Thresholds\Connection** menu.

No Responses

The **No Responses** threshold specifies the number of consecutive retransmissions in the same direction on a single connection without response that implies a connection is broken. For example, if **No responses** has been set to 3 (the default), the analyzer will diagnose that a connection is lost after a packet has been retransmitted 3 times. The analyzer will generate both a diagnosis and a symptom message. The message is **Non-responsive station:** ***Station name***.

Possible values range from 0 to 999; default value is 3.

Retransmission Percentage

The **Retransmission Percentage** threshold specifies the maximum acceptable percentage of retransmitted packets versus successfully transmitted packets in the same direction on a single connection at the Connection layer. If this percentage is exceeded, the analyzer generates the diagnosis **Retransmissions**. The value for **Retrans %** is calculated as follows:

Number of retransmitted packets / Number of non-retransmitted packets *x* 100

Possible values range from 0 to 100 percent; default value is 10 percent.

Zero Window

The **Zero Window** threshold specifies the duration of a zero window before the analyzer displays the symptom message, **Zero window for *x* seconds**. A network station receiving data notifies the sender of its buffer size (the window size). A zero window indicates that the receiver's buffer is full. Transmission to this station stops until it sends a non-zero window advertisement.

The threshold value is the time between a zero window advertisement and the subsequent non-zero window advertisement.

Possible values range from 0 to 999 seconds; default is 5 seconds.

Idle Timer

The **Idle Timer** threshold specifies in minutes the maximum time a connection at the Expert Connection layer can remain idle. A connection is considered idle if no packets are sent in either direction. If the idle time of a given connection exceeds the **Idle Timer** value, the analyzer generates the symptom **Idle more than *x* minutes**.

Possible values range from 0 to 999 minutes; default value is 10 minutes.

Fast Retransmission

The **Fast Retransmission** threshold specifies the minimum time between packet retransmissions. If a station retransmits a packet before the analyzer's **Fast retrans** timer has expired, the analyzer generates the symptom **Retransmission with too short timer**.

Possible values range from 0 to 999 milliseconds; default value is 100 milliseconds.

TCP Keep Alive

The **TCP Keep Alive** threshold is used to specify whether a retransmitted frame represents a real retransmission or a "keep alive" frame. For example, if **TCP keep alv** is set to 10 seconds, a frame retransmitted less than 10 seconds after its first transmission is not considered a TCP keep alive.

Possible values range from 0 to 999 seconds; default is 25 seconds.

DEC Keep Alive

The **DEC Keep Alive** threshold is used to specify whether a retransmitted frame represents a real retransmission or a "keep alive" frame. For example, if **DEC keep alv** is set to 10 seconds, a frame retransmitted more than 10 seconds after its first transmission is considered a DEC keep alive.

Possible values range from 0 to 999 seconds; default is 5 seconds.

Network Station Thresholds

The Expert thresholds in this section refer to symptoms and diagnoses at the Network layer. Symptoms and diagnoses at the Network layer are associated with network addressing and routing problems. The thresholds are organized as they are found in the **Expert settings\Thresholds\Network Station** menu.

Multiple Routers

The **Multiple Routers** threshold specifies the maximum number of local routers through which local traffic can be routed to a remote station. If there are more routers than specified, the analyzer displays the diagnosis **Multiple routers to station** ***station name***.

Possible values range from 0 to 10; default is 3.

DEC Hello

If the DECnet hello timer is less than the value specified for **DEC hello,** the analyzer will trigger the symptom **Small hello time**.

DECnet uses hello packets for neighbor identification. In a DECnet environment, a station needs to know of at least one intermediate system (a router) to which it can hand off packets with unknown destinations. Hello packets let a station find this default intermediate system. The DECnet hello timer controls how often hello packets are sent. Because hello packets contribute to network overhead, the hello timer should be set as high as possible, depending on the stability of the environment. A short hello timer can lead to high network traffic and routing problems.

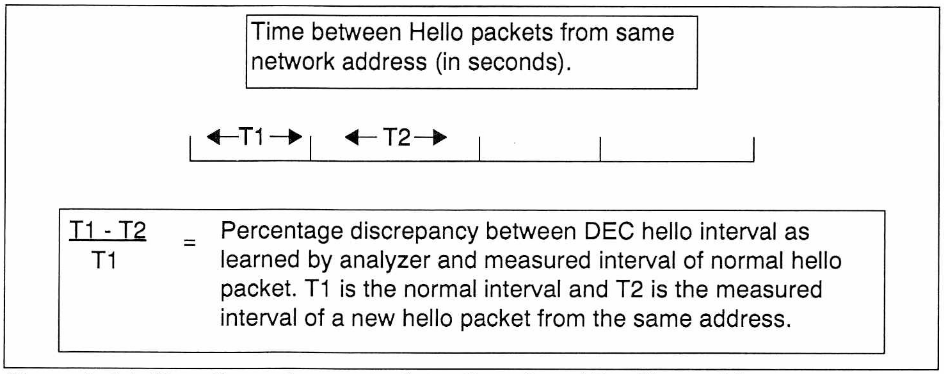
Possible values range from 0 to 999 seconds; default is 10 seconds.

Duplicate Percentage

The Expert analyzer uses several different algorithms to detect the presence of duplicate network addresses on the network. The **Duplicate address percentage** threshold allows you to fine-tune the algorithm specific to the DECnet environment.

In the DECnet environment, stations are required to send a hello packet at a specified time interval (for an explanation of the DEC Hello packet, see, "DEC Hello," above). The analyzer uses these hello packets to detect duplicate network addresses. Because the time between hello packets for a given station should theoretically remain a constant, the analyzer will generate a **Duplicate net address** diagnosis if it detects a discrepancy in the intervals for hello packets sent from a single network address. Because of fluctuations in the intervals of hello packets with the same network address, the analyzer assumes that two different stations are sending hello packets with the same network address.

Theoretically, the interval between hello packets for a given network station should remain constant. However, due to various network irregularities, the interval tends to vary within a small range of the specified interval. As capture proceeds, the analyzer "learns" the usual interval for hello packets from a given station. The **Duplicate address percentage** threshold specifies the maximum percentage discrepancy between the usual DEC hello interval as learned by the analyzer and the measured DEC hello interval of a given frame. Figure 3–14 illustrates the concept of the **Duplicate address percentage** threshold.


Time between Hello packets from same network address (in seconds).
←T1→
←T2→

$\frac{T1 - T2}{T1}$ = Percentage discrepancy between DEC hello interval as learned by analyzer and measured interval of normal hello packet. T1 is the normal interval and T2 is the measured interval of a new hello packet from the same address.

Figure 3–14. How the analyzer calculates the value of Duplicate address percentage.

If your network is very busy, or has a lot of "noise," you may want to set the Duplicate address percentage threshold at a high percentage to avoid spurious **Duplicate Network Address** diagnoses. Possible values range from 0 to 100 percent; the default is 10 percent.

DLC Station Thresholds

This section describes the Expert thresholds related to symptoms and diagnoses detected at the Expert Data Link layer. Symptoms and diagnoses at the Data Link layer are associated with problems such as broadcast storms and traffic bursts. The thresholds are organized as they are found in the **Expert settings\Thresholds\DLC Station** menu. Token ring-specific (MAC level) thresholds are described starting on page 3–26. WAN/Synchronous-specific thresholds are described starting on page 3–28.

LAN Overload

The **LAN Overload** threshold specifies the network load at which the analyzer should generate a **Network overload** symptom. Network load is measured as a percentage of maximum bandwidth.

Possible values range from 1 to 100 percent; default is 30 percent for Ethernet and 60 percent for token ring.

Because of the token-passing nature of token ring networks, collisions are non-existent. Network loads can therefore remain trouble-free at higher volumes on token ring than on Ethernet. This explains the difference in default values for the **Network overload** threshold.

LAN Overload Percentage

The **LAN Overload Percentage** threshold specifies at what point the analyzer diagnoses that the network is overloaded. The diagnosis is **Overloaded network.**

LAN overload % is measured as the percentage of each minute the network is in overload mode. Whether the network is considered to be in overload mode depends on the setting of **LAN overload.**

Figure 3–15 illustrates the relationship between **LAN overload** and **LAN overload %**. In this example, the threshold **LAN overload** is defined as traffic greater than 30 percent of maximum bandwidth, and the threshold **LAN overload %** is defined as 20 percent. The total number of seconds during which the network experiences an overload is about 20. That is, the network is in overload mode for 30 percent of the time during this minute, which is higher than the **LAN overload percentage** threshold (20 percent). The analyzer diagnoses that the network is overloaded.

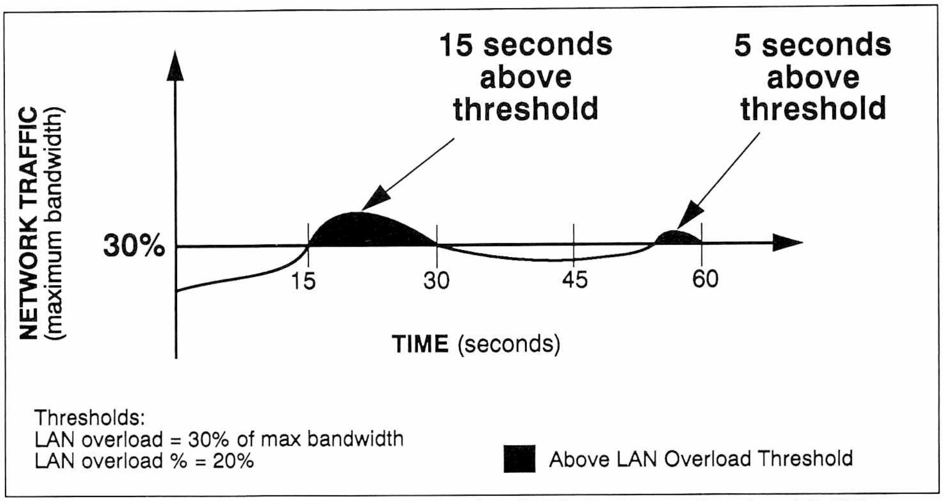


Figure 3–15. The relationship between the thresholds ***LAN overload*** *and* ***LAN overload%****.*

Broadcast Symptom

The **Broadcast Symptom** threshold specifies the rate of broadcast/multicast packets per second above which the analyzer will generate the symptom **Broadcast/Multicast storm.**

Possible values range from 0 to 999; default value is 40 broadcast packets per second.

Broadcast Diagnosis

The **Broadcast Diagnosis** threshold specifies the rate of broadcast/multicast packets per second above which the analyzer will generate the diagnosis **Broadcast storm**.

Characteristically, the value chosen to trigger a broadcast storm *diagnosis* (**Broadcast dg**) will be greater than that chosen to trigger a broadcast storm *symptom* (**Broadcast sy**).

Possible values range from 0 to 999; default value is 120 broadcast packets per second.

Physical Errors

The **Physical Errors** threshold specifies the maximum acceptable number of physical errors per second per station.

If the number of frames with physical errors sent by a given station exceeds the threshold, the analyzer generates the diagnosis **High rate of physical errors by** ***station name***.

Note: The analyzer also tracks the number of physical error frames received by each station. However, this quantity does not affect when the **High physical level error rate** diagnosis is generated.

Possible values are 0 to 999 errors per second; default value is 4 errors per second per station.

Token Ring-Specific (MAC level) Thresholds

This section describes Expert thresholds that are specific to token ring; particularly, thresholds relating to the MAC level. The Expert analyzer captures and decodes all MAC level (including Report Soft Error) frames on the ring, providing accurate detection of token ring symptoms and diagnoses.

The thresholds are organized in the same order they are found in the **Expert settings\Thresholds\DLC Station** menu.

Ring Entries

The **Ring Entries** threshold specifies the rate of ring entries per minute per station at which the analyzer will generate the **High rate of ring entries** diagnosis. For example, if **Ring entries** is set to 2 (the default), the analyzer will generate the diagnosis when the rate of ring entries for a particular station equals or exceeds two per minute.

A station inserting to a ring physically "breaks" the ring as its relay in the multistation access unit (MAU) opens and the lobe becomes part of the ring. The ring recovers quickly, as this is normal token ring behavior. However, it is abnormal if there is more than one ring entry per minute for a given station. Default values are set accordingly.

Possible values are 0 to 999 ring entries per minute; default value is 2 per minute.

RX Congestion (Receiver Congestion)

The **RX Congestion** threshold specifies the rate of receiver congestion errors per minute per station at which the analyzer will generate the **High rate of receiver congestion** diagnosis. For example, if **RX congestion** is set to 60 (the default), the analyzer will generate the diagnosis when the rate of receiver congestion errors for a particular station equals or exceeds 60 per minute.

Receiver congestion errors indicate that a station detected a frame on the ring with its own destination address but was unable to copy it because it had no buffer space available. A new receiver congestion error is generated each time a new frame is rejected. Receiver congestion errors can be important guides when judging the adequacy of current servers and gateways on the ring. An abundance of receiver congestion errors from an interconnecting device may point to its obsolescence.

Possible values are 0 to 999 receiver congestion errors per minute. Default is 60 receiver congestion errors per minute.

Station Removed

The **Station Removed** threshold specifies the rate of Station Remove Requests per minute at which the analyzer will generate the diagnosis **High rate of remove from ring requests.** For example, if Station Remove is set to 1 (the default), the analyzer will generate the diagnosis when the rate of Station Remove Requests detected by the analyzer exceeds one per minute.

Station Remove Requests are sent by the Configuration Report Server, a virtual entity responsible for the overall health of the ring.

Possible values are 1 to 999 requests per minute. Default is 1 request per minute.

Ring Errors

The **Ring Errors** threshold specifies the rate of ring errors per minute per station at which the analyzer will generate the diagnosis **High rate of line/burst errors**. The threshold specifies the total of both line errors and burst errors per minute. For example, if **Ring errors** was set to three, the analyzer would generate the **High rate of line/burst errors** diagnosis when the rate of total line and burst errors for a given station exceeded three per minute.

Possible values are from 0 to 999 ring errors per minute. Default is 1 ring error per minute.

Ring Purge Symptom

The **Ring Purge Symptom** threshold specifies the rate of ring purges per station per minute at which the analyzer will generate the symptom **High rate of ring purges**. Ring purge frames are sent by the active monitor when it detects that a token has been lost, and are part of normal token ring behavior. However, an excessive amount of ring purge frames on the network can indicate potential hardware problems.

Possible values are from 0 to 999 ring purge frames per minute. Default is 30 ring purge frames per minute.

Note: When the **Ring purge sy** threshold is exceeded, the analyzer generates a *symptom*. The analyzer generates a *diagnosis* when the **Ring purge dg** threshold is exceeded. See below.

Ring Purge Diagnosis

The **Ring Purge Diagnosis** threshold specifies the rate of ring purges per station per minute at which the analyzer will generate the diagnosis **High rate of ring purges**. For a brief description of ring purge frames, see the section, "Ring Purge Symptom," above.

Characteristically, the value chosen to trigger a **High rate of ring purges** *diagnosis* (**Ring purge dg**) will be greater than that chosen to trigger a **High rate of ring purges** *symptom* (**Ring purge sy**).

Possible values are from 0 to 999 ring purge frames per minute. Default is 60 ring purge frames per minute.

WAN/Synchronous (Sniffer Internetwork Analyzer) Thresholds

This section describes those Expert thresholds that are specific to the Sniffer Internetwork Analyzer (that is, the Sniffer analyzer for WAN/Synchronous).

The thresholds are organized in the same order they are found in the **Expert settings\Thresholds\DLC station** menu.

WAN Overload

The **WAN Overload** threshold works in tandem with the **Overload Timer** threshold to specify the point at which the analyzer generates the **Network Overload** symptom and the **Overloaded Network** diagnosis.

The **WAN Overload** threshold specifies whether the Expert analyzer considers the network to be in an overload condition. The Expert analyzer considers the network to be in an overload condition if both the DTE and DCE network loads are in excess of the load specified by the **WAN Overload** threshold. The Expert analyzer will continue to consider the network to be in an overload condition until either the DTE or DCE network load falls below the load specified by the **WAN Overload** threshold.

When the duration (in consecutive seconds) of the overload condition exceeds the time specified by **Overload Timer** (below), the analyzer will generate the **Network Overload** symptom (in the Global Symptoms view) and the **Overloaded Network** diagnosis.

Possible values range from 1 to 100 percent; default is 80 percent.

Overload Timer

The **Overload Timer** threshold works in tandem with the **WAN Overload** threshold to specify the point at which the analyzer diagnoses that the WAN is overloaded. The diagnosis is **Overloaded Network.**

The **Overload Timer** threshold specifies the duration (in seconds) of a WAN Overload condition at which the Expert analyzer will generate an **Overloaded Network** diagnosis. Whether the network is considered to be in an overload condition depends on the setting of the **WAN Overload** threshold.

Possible values range from 1 to 999 seconds; default is 60 seconds.

WAN Underload

The **WAN Underload** threshold works in tandem with the **Underload Timer** threshold to specify the point at which the analyzer generates the **Network Underload** symptom and the **Underloaded Network** diagnosis.

The **WAN Underload** threshold specifies whether the Expert analyzer considers the network to be in an underload condition. The Expert analyzer considers the network to be in an underload condition if both the DTE and DCE network loads are below the load specified by the **WAN Underload** threshold. The Expert analyzer will continue to consider the network to be in an underload condition until either the DTE or DCE network load increases above the load specified by the **WAN Underload** threshold.

When the duration (in consecutive minutes) of the underload condition exceeds the time specified by **Underload Timer** (below), the analyzer will generate the **Network Underload** symptom (in the Global Symptoms view) and the **Underloaded Network** diagnosis.

Possible values range from 0 to 100 percent; default is 10 percent.

Underload Timer

The **Underload Timer** threshold works in tandem with the **WAN Underload** threshold to specify the point at which the analyzer diagnoses that the WAN is underloaded. The diagnosis is **Underloaded Network**.

The **Underload Timer** threshold specifies the duration (in minutes) of a WAN Underload condition at which the Expert analyzer will generate an **Underloaded WAN** diagnosis. The setting of **WAN Underload** determines whether or not the network is considered to be in an underload condition.

Possible values range from 1 to 999 minutes; default is five minutes.

Congestion Percentage

The Congestion Percentage threshold specifies the point at which the analyzer will generate congestion-related symptoms. The Congestion Percentage threshold is calculated differently depending on the type of access protocol used by the WAN link to which the analyzer is attached.

Frame Relay

There are two Frame Relay congestion symptoms:

- **Excessive Forward Congestion**. The Expert analyzer generates this symptom when the percentage of forward explicit congestion notification (FECN) frames to total frames on the link exceeds the percentage specified by the **Congestion Percentage** threshold.
- **Excessive Backward Congestion**. The Expert analyzer generates this symptom when the percentage of backward explicit congestion notification (BECN) frames to total frames on the link exceeds the percentage specified by the **Congestion Percentage** threshold.

HDLC

On an HDLC link, the Expert analyzer generates the **Overcongested WAN** symptom when the percentage of receiver not ready (RNR) frames to

RNR+Receiver Ready (RR) frames exceeds the **Congestion Percentage** threshold.

Possible values range from 0 to 100 percent; default is 10 percent.

Effects of Changing Expert Thresholds

When you display frames after changing any of the Expert thresholds, the analyzer automatically reanalyzes the frames in the capture buffer. During analysis, the Expert analyzer uses the new Expert settings to generate symptom and diagnosis messages.

WARNING: When the Expert reanalyzes the frames in the capture buffer, it releases all the network objects it has created, including those gleaned from frames no longer in the capture buffer. The results of post-capture Expert analysis will be based solely on information found in the frames currently in the capture buffer. Once network objects associated with frames outside of the capture buffer have been released, they cannot be regained.

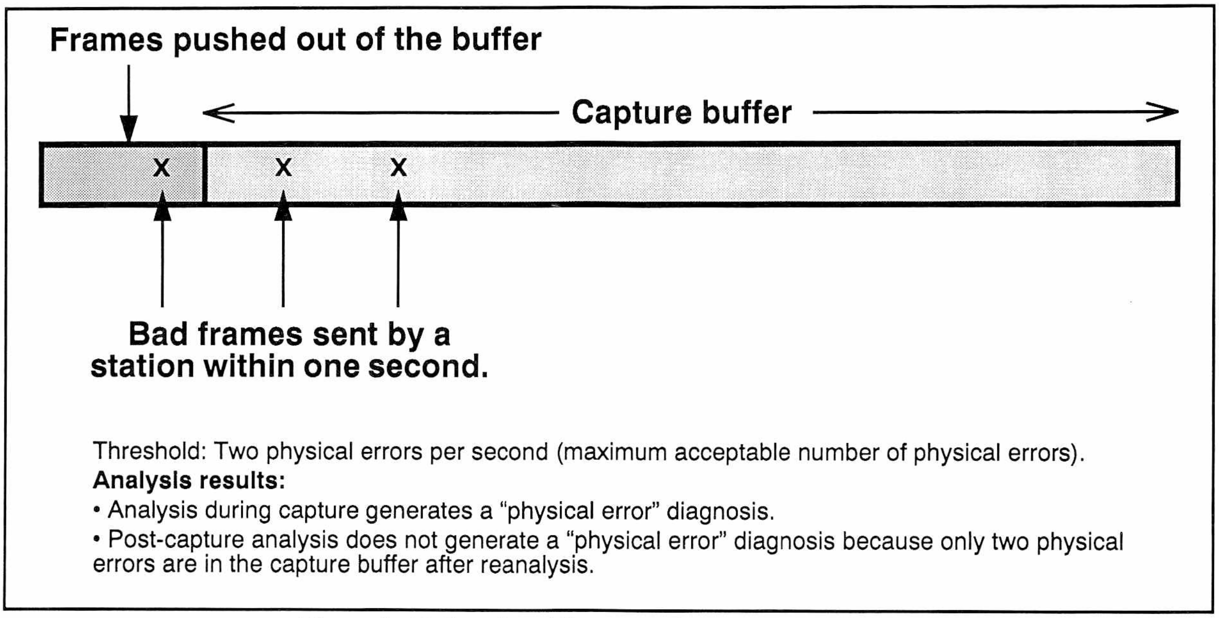
Changing the Expert settings will most likely change the results of Expert analysis on a given set of network data. There are at least two ways changing an Expert threshold will affect the results of Expert analysis:

- A modified threshold doesn't affect the captured data, but the analysis results change because previously analyzed frames are no longer in the capture buffer.
- A modified threshold is relevant to the data currently in the capture buffer. If this is the case, lowering the Expert thresholds will generally increase the number of symptom or diagnosis messages.

The examples below illustrate each of these possibilities.

Example One: Changing a Threshold Irrelevant to the Data in the Capture Buffer

Figure 3–16 illustrates the effect reanalyzing a subset of the frames that have passed through the capture buffer can have on the results of Expert analysis. In this example, the **Physical errors** threshold was set to two for both the original capture session as well as the post-capture analysis. During the original capture session, the analyzer generates the **Physical error** diagnosis when the threshold is exceeded. However, during post-capture analysis, a frame exhibiting one of the physical errors is now outside of the capture buffer. Because the analyzer no longer knows of the existence of that frame, the threshold is not exceeded, and no diagnosis is generated.


Frames pushed out of the buffer
Capture buffer
X
X
X
Bad frames sent by a station within one second.

Threshold: Two physical errors per second (maximum acceptable number of physical errors).
Analysis results:
- Analysis during capture generates a "physical error" diagnosis.
- Post-capture analysis does not generate a "physical error" diagnosis because only two physical errors are in the capture buffer after reanalysis.

Figure 3–16. Results of Expert analysis can vary depending on when performed.

Example Two: Changing a Threshold Relevant to the Data in the Capture Buffer

In some cases, the effect of a modified Expert threshold is not as obvious. Consider the following example:

You are capturing frames from a trace file and analyzing with the data link threshold settings as follows:

- **LAN overload** = 30% (percentage of available bandwidth)
- **LAN overload %** = 20
- **Broadcast sy** = 2
- **Broadcast dg** = 1
- **Physical err** = 4

Under these data link thresholds, the analyzer detects a broadcast storm symptom after capturing frame 38 at 16:18:14.3693.

Suppose you capture again from the same file with this new threshold setting:

- **LAN overload**= 8%

Although the thresholds related to broadcast storms remain unchanged, the new analysis results show no broadcast storm symptoms or diagnoses. Instead, the analyzer detects a Network overload symptom at 16:18:13.7949.

What happened? With the decreased threshold for **LAN overload**, it became much easier to trigger a Network overload symptom. Frame 38 captured at 16:18:13.7949 exceeded the new threshold for **LAN overload**, and the analyzer alerted us to a LAN overload symptom. The analyzer never realized that Frame

38 also exceeded the **Broadcast sy** threshold. Because the analyzer stops analyzing a frame after detecting the first symptom or diagnosis associated with a frame, it is possible that a frame has more than one symptom, and the analyzer only displays a message for the first symptom or diagnosis detected.

Figure 3–17 illustrates the time passage between the detection of the two symptoms.

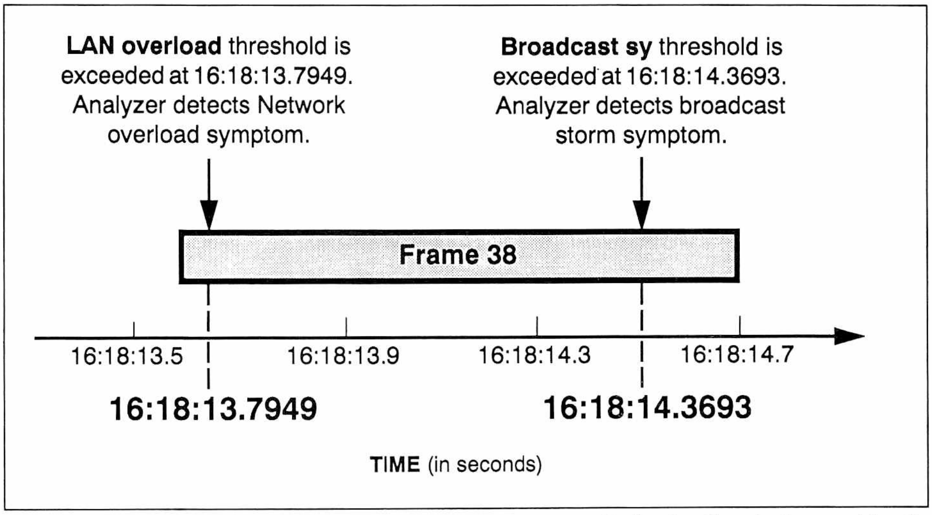

LAN overload threshold is exceeded at 16:18:13.7949. Analyzer detects Network overload symptom.
Broadcast sy threshold is exceeded at 16:18:14.3693. Analyzer detects broadcast storm symptom.
Frame 38
16:18:13.5
16:18:13.9
16:18:14.3
16:18:14.7
16:18:13.7949
16:18:14.3693
TIME (in seconds)

Figure 3–17. A single frame exhibiting two symptoms. Only the first is detected by the analyzer.

Console Alarms

This section describes the meaning of each user-defined alarm. Depending on the topologies you ordered from the factory, the exact alarms available on your analyzer may be a subset of those described here. Figure 3–18 shows the available alarms at each Expert layer. The alarms are described in the same order in which they appear in the analyzer's menus.

Expert Layer	Alarm Generated	Related Expert Threshold
Application Layer	Slow File Process	Slow File Percentage
	Slow Server	Slow Response Percentage
	Loop On Requests	Loop Time Percentage
	File Retransmission	Slow File Percentage
	Requests Denied	Denied Count/Denied Request Percentage
Connection Layer	Broken Connection	No Responses
	Retransmission	Retransmission Percentage
Network Layer	Duplicate Address	Duplicate Percentage
	Local Router	
	Multiple Router	Multiple Router
DLC Station Layer	Network Overload	LAN Overload Percentage
	Broadcast Storm	Broadcast Diagnosis
	Physical Error	Physical Error Count
MAC Layer (Token Ring)	Token Ring Entries	Ring Entries
	Ring Purges	Ring Purge Diagnosis
	Token Ring Bursts	Ring Errors
	Receive Congestion Burst	Receive Congestion Error Count
	Station Removed	Station Removed Count
	Beacon	

Figure 3–18. Alarm Priorities available for each Expert layer.

Application Layer Alarms

The alarms at the Expert application layer are described in this section in the same order they appear in Figure 3–18. Note that these alarms are generated based on related Expert thresholds specified in the **Expert settings\Thresholds** menu. For information on these related Expert thresholds, refer to the section, "Symptom and Diagnosis Thresholds at Each Expert Layer," beginning on page 3–15.

Slow File Process

The **Slow File Process** alarm is generated to the Console based on the **Slow File Percentage** threshold. The **Slow File Percentage** threshold specifies the maximum percentage of slow file transfers versus total file transfers. An alarm is also generated to the Console when the **Local Transfer** or **Remote Transfer** threshold settings have been exceeded.

The default setting is **Warning**.

Slow Server

The **Slow Server** alarm is generated to the Console based on the **Slow Response Percentage** threshold. The **Slow Response Percentage** threshold determines whether the analyzer considers a server slow in responding to application requests. An alarm is also generated to the Console when the **Response Time** threshold has been exceeded.

The default setting is **Major**.

Loops on Requests

The **Loops on Request** alarm is generated to the Console based on the **Loop Percentage** threshold. The **Loop Percentage** threshold specifies the ratio between repeated requests and normal requests.

The default setting is **Inform**.

File Retransmissions

The **File Retransmissions** alarm is generated to the Console based on the **Slow File Percentage** threshold. The **Slow File Percentage** threshold specifies the maximum percentage of file retransmissions versus normal file transfers for a given connection.

The default setting is **Inform**.

Requests Denied

The **Requests Denied** alarm is generated to the Console based on the **Denied Count** and **Denied Request Percentage** thresholds that specify the maximum number of denied requests and the acceptable percentage of denied versus successful application requests for a given application.

An alarm is also generated to the Console when the **Filter Time** threshold has been exceeded.

The default setting is **Warning**.

Connection Layer Alarms

The alarms at the Expert connection layer are described in this section in the same order they appear in Figure 3–18. Note that these alarms are generated based on related Expert thresholds specified in the **Expert settings\Thresholds** menu. For information on these related Expert thresholds, refer to the section, "Symptom and Diagnosis Thresholds at Each Expert Layer," beginning on page 3–15.

Broken Connection

The **Broken Connection** alarm is generated to the Console based on the **No Responses** threshold that specifies the maximum number of consecutive retransmissions in the same direction on a single connection without a response.

The default setting is **Inform**.

Retransmission

The **Retransmission** alarm is generated to the Console based on the **Retransmission Percentage** threshold. The **Retransmission Percentage** threshold specifies the maximum acceptable percentage of retransmitted packets versus successfully transmitted packets in the same direction on a single connection at the connection layer.

The default setting is **Major**.

Network Layer Alarms

The alarms at the Expert network layer are described in this section in the same order they appear in Figure 3–18. Alarms generated at the network layer are associated with network addressing and routing problems. Note that these alarms are generated based on related Expert thresholds specified in the **Expert settings\Thresholds** menu. For information on these related Expert thresholds, refer to the section, "Symptom and Diagnosis Thresholds at Each Expert Layer," beginning on page 3–15.

Duplicate Address

The **Duplicate Address** alarm is generated to the Console based on the **Duplicate Percentage** threshold that specifies the maximum percentage discrepancy between DEC hello intervals.

The default setting is **Critical**.

Local Router

The **Local Router** alarm is generated to the Console when a router forwards local traffic. The default setting is **Minor.**

Multiple Routers

The **Multiple Routers** alarm is generated to the Console based on the **Multiple Routers** threshold. The **Multiple Routers** threshold specifies the maximum number of local routers through which local traffic can be routed to a remote station.

The default setting is **Inform**.

DLC Station Layer Alarms

The alarms at the Expert data link layer are described in this section in the same order they appear in Figure 3–18. Alarms generated at the data link layer are associated with problems such as broadcast storms and traffic bursts. Note that these alarms are generated based on related Expert thresholds specified in the **Expert settings\Thresholds** menu. For information on these related Expert thresholds, refer to the section, "Symptom and Diagnosis Thresholds at Each Expert Layer," beginning on page 3–15.

Network Overload

The **Network Overload** alarm is generated to the Console based on the **LAN Overload Percentage** threshold. The **LAN Overload Percentage** threshold specifies at what point the analyzer diagnoses that the network is overloaded.

The default setting is **Minor.**

Broadcast Storm

The **Broadcast Storm** alarm is generated to the Console based on the **Broadcast Diagnosis** threshold that specifies the rate of broadcast and multicast packets per second above which the analyzer generates the Broadcast storm diagnosis.

The default setting is **Minor.**

Physical Error

The **Physical Error** alarm is generated to the Console based on the **Physical Error Count** threshold that specifies the maximum acceptable number of physical errors per second per station.

The default setting is **Major.**

Token Ring-Specific (MAC level) Alarms

This section describes those alarms specific to token ring; particularly, those alarms relating to the MAC level. Note that these alarms are generated based on related Expert thresholds specified in the **Expert settings\Thresholds** menu. For information on these related Expert thresholds, refer to the section, "Symptom and Diagnosis Thresholds at Each Expert Layer," beginning on page 3–15.

Token Ring Entries

The **Token Ring Entries** alarm is generated to the Console based on the **Ring Entries** threshold that specifies the rate of ring entries per minute per station above which the analyzer generates the High rate of ring entries diagnosis.

The default setting is **Minor**.

Ring Purges

The **Ring Purges** alarm is generated to the Console based on the **Ring Purge Diagnosis** threshold that specifies the rate of ring purges per station per minute above which the analyzer generates the High rate of ring purges diagnosis.

The default setting is **Minor**.

Token Ring Bursts

The **Token Ring Bursts** alarm is generated to the Console based on the **Ring Errors** threshold that specifies the rate of ring errors per minute per station above which the analyzer generates the High rate of line/burst errors diagnosis.

The default setting is **Inform**.

Receive Congestion Burst

The **Receive Congestion Burst** alarm is generated to the Console based on the **Receiver Congestion** threshold that specifies the rate of receiver congestion errors per minute per station above which the analyzer generates the High rate of receiver congestion diagnosis.

The default setting is **Major**.

Station Removed

The **Station Removed** alarm is generated to the Console based on the **Station Removed** threshold that specifies the rate of Station Remove Requests per minute above which the analyzer generates the High rate of remove from ring requests diagnosis.

The default setting is **Minor**.

Beacon

The Beacon alarm is generated to the Console when the Server is in a beaconing state. The default setting is **Critical**.

Alarm Levels

The alarm level of the Server is indicated on the Console's Server Status screen. This indicates the highest priority alarm detected by the Server. To lower the alarm level on a Monitor Server, you must acknowledge or clear the alarm on the Server.

For Expert Servers, the alarm level indicates the highest level alarm currently active on the Server. As new diagnoses are generated or go active, the alarm level is raised if the diagnosis is of higher priority than the current alarm level. The alarm level will be lowered when the highest active alarm on the Server has been lower than the Server alarm level for some amount of time. This amount of time may be set between 1 and 5940 minutes (that is, up to 99 hours) from the **Expert settings\Level timer** menu. The default setting is five minutes.

To set the alarm level:

1. Move to the **Expert settings\Level timer** = field.
2. Press Enter.

   A dialog box is displayed with the current setting.
3. Enter the amount of time you want between 1 and 5940 minutes and press Enter.

Alarm Throttle

Diagnoses are triggered by some threshold level of symptom. When the symptom level is near the configured threshold for triggering a diagnosis, you may see the diagnosis toggling between active and inactive states. An alarm is sent to the Console on each transition into the active state.

Alarm throttle allows you to configure the Server to not send an alarm about the same diagnosis more than once every x minutes, where x can range from zero to 5940 minutes (that is, up to 99 hours). The default setting is one minute.

To configure the alarm throttle:

1. Move to the **Expert settings\Throttle** = field.
2. Press Enter.

   A dialog box is displayed with the current setting.
3. Enter the amount of time you want between 0 and 5940 minutes and press Enter.

Expert Triggers

Expert triggers allow you to use diagnoses as trigger events, anchoring capture to make sure the frames that interest you are either saved to hard disk as a snapshot or remain in the capture buffer. This section describes the mechanics of setting an Expert trigger. It does not discuss in detail the meanings of the triggers, which are described in the next few sections.

You can specify an Expert trigger along with external and pattern triggers. If you use these different types of triggers, you should read "The Order in Which the Analyzer Processes Triggers" on page 3–42 to understand how the analyzer processes triggers.

To set an Expert trigger:

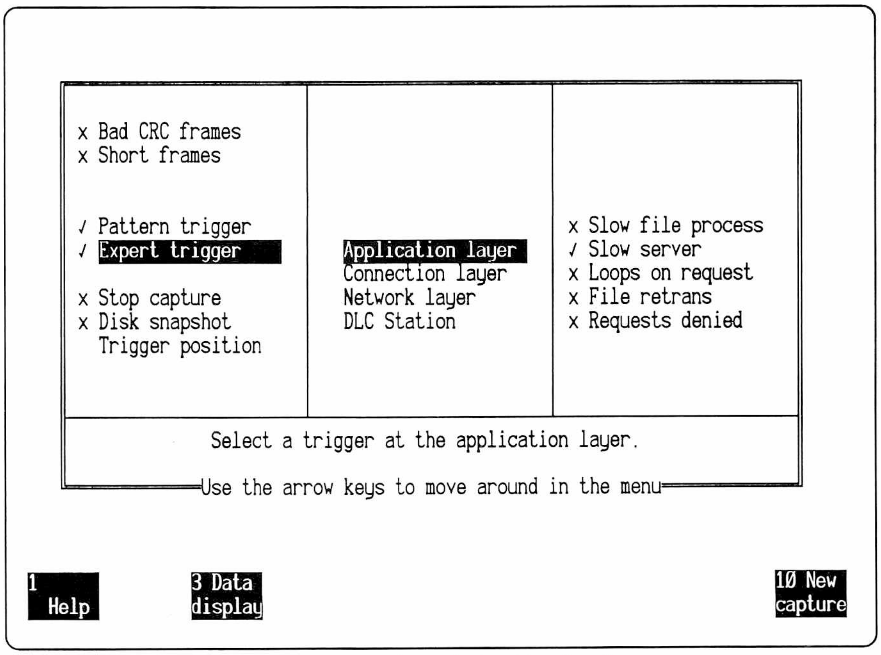
1. Use the cursor keys to move to the **Trigger\Expert Trigger** menu.
2. Move the highlight to the layer at which you want to specify an Expert trigger.

   Result: A list of Expert triggers associated with the highlighted layer appears in the right menu panel. Figure 3–19 shows the Expert triggers associated with the Application layer.

In Figure 3–19, notice that each Expert trigger is preceded by either an x or a √. Triggers preceded by a √ are enabled; those preceded by an x are disabled. You can use the Spacebar to toggle between enabled/disabled. By pressing alt-Spacebar, you can reverse all selections in the current display.

3. Move the highlight to a trigger you want to enable. Press the Spacebar to change its tag from an x (disabled) to √ (enabled). Repeat this process for each trigger you want to enable or disable. In Figure 3–19, the Expert trigger **Slow server** is enabled.
4. In Figure 3–19, the menu item **Expert trigger** is also preceded by a √. You can enable or disable all Expert triggers as a group.
5. Set other trigger options, such as **Stop capture**, **Disk snapshot**, and **Trigger position**. For more information on these options, see the *Distributed Sniffer System: Analyzer Operations Manual.*
6. Press F10 (**New capture**) to start capture.

   Result: When capture begins, the new trigger takes effect.



```
x Bad CRC frames
x Short frames

✓ Pattern trigger
✓ Expert trigger          Application layer     x Slow file process
                          Connection layer      ✓ Slow server
x Stop capture            Network layer         x Loops on request
x Disk snapshot           DLC Station           x File retrans
  Trigger position                              x Requests denied

              Select a trigger at the application layer.
           Use the arrow keys to move around in the menu

1      3 Data                                              10 New
 Help  display                                             capture
```

Figure 3–19. The Trigger \ Expert trigger \ Application layer menu.

Effects of an Expert Trigger

The frame causing an Expert trigger is marked with a T in the summary view. The diagnosis was probably not caused by the marked frame alone. The mark simply indicates where the diagnosis is made. For example, if you set the diagnosis **Broadcast storm** to be the trigger event, the trigger frame indicates at what time the analyzer decided that a broadcast storm happened; it doesn't mean that the frame itself caused a broadcast storm.

After an Expert trigger occurs, the analyzer does the following:

- Emits a beep, notifying you that a trigger event has occurred.
- Continues or stops capture, depending on the settings of **Stop capture** and **Trigger position**.

  If **Stop capture** is disabled, the analyzer continues capturing, and it is possible that the frame associated with an Expert trigger could be pushed out of the buffer by the time you stop capture.

  If **Stop at trigger** is selected, the analyzer continues capturing until the frame associated with the Expert trigger is in the position described by **Trigger position**. For example, if **Trigger position** is 100 percent pretrigger, capture stops immediately after the trigger event has happened. In this case, the related alarm will not be sent to the Console and any other alarms queued but not yet sent will not be sent to the Console.

  If **Stop when full** is selected, the analyzer continues capturing until the buffer is full. If a trigger event occurs, the trigger frame remains in the buffer, but its relative position is not predetermined.

- If **Disk snapshot** is selected, the analyzer stores the frames surrounding the trigger event to the disk. Depending on the configuration of the various **Disk snapshot** options, the analyzer can either continue capturing or stop after the first trigger. Refer to the *Distributed Sniffer System: Analyzer Operations Manual* for further information on how disk snapshots are taken.

For general information on setting and manipulating triggers, refer to the *Distributed Sniffer System: Analyzer Operations Manual.*

Available Expert Triggers

The Expert triggers are organized by Expert layers, each of which contains several trigger options. Figure 3–20 summarizes the Expert triggers available at each Expert layer.

Expert Layer	Expert Threshold
Application Layer	Slow file process
	Slow server
	Loops on request
	File retransmission
	Requests denied
Connection Layer	Broken connection
	Retransmission
Network Station Layer	Duplicate address
	Local router
	Multiple routers
	Subnet down
	Bad routing table
	Subnet conflict

Figure 3–20. Expert triggers available at each Expert layer.

Expert Layer	Expert Threshold
DLC Station Layer	Overloaded LAN
	Broadcast storm
	Physical error
	Overloaded WAN
	WAN underload*
	HDLC retransmits*
	Overcongested WAN*
	Underload congestion*
MAC Layer (Token Ring)	Token ring entry
	Ring purge
	Receiver congestion
	Station removed
	Beaconing ring
	Token ring burst

*Sniffer Internetwork Analyzer (WAN/Synchronous) only

Figure 3–20. Expert triggers available at each Expert layer.

The Order in Which the Analyzer Processes Triggers

Normally, if you specify multiple triggers, whichever frame that fulfills a trigger condition first is considered the trigger frame and is marked with a T.

However, if you specify both Classic and Expert triggers, it is possible that the analyzer will ignore the Expert trigger event even though it precedes the Classic event. This is because the analyzer processes Classic triggers faster than Expert triggers. The following example explains this concept.

Example: Processing Expert and Classic Triggers

Suppose you specify one Classic pattern-match trigger and one Expert trigger. In Figure 3–21, frame 90 fulfills the condition of the Expert trigger and frame 100 fulfills that of the pattern-match trigger. Because the analyzer processes the Classic pattern-match trigger on frame 100 before it performs Expert analysis on frame 90, frame 100 is marked as the trigger frame instead of frame 90. The analyzer does not consider frame 90 to be the first trigger event. As a result, you might not be aware that a frame associated with the Expert trigger has ever occurred.

You can avoid this problem by enabling only Expert triggers. If no Classic triggers are enabled, you are assured that the analyzer will recognize the Expert trigger event accurately.

Two triggers are set:
Pattern-match trigger – Trigger on a frame reporting an SMB error.
Expert trigger – Trigger on a frame that is retransmitted at the transport layer.

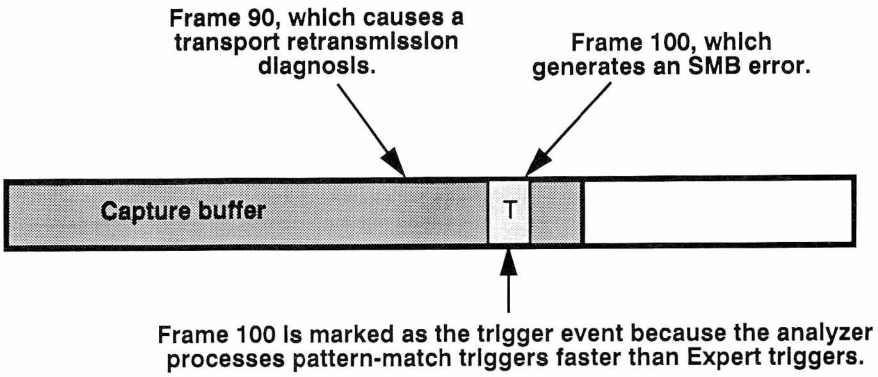

Frame 90, which causes a transport retransmission diagnosis.
Frame 100, which generates an SMB error.
Capture buffer
T
Frame 100 is marked as the trigger event because the analyzer processes pattern-match triggers faster than Expert triggers.

Figure 3–21. The order in which the analyzer processes triggers.

Customizing a Capture Session

You can customize an Expert capture session by specifying the screen format, capture filters, frame size, and so on. In addition, there are several Expert-specific options which allow you to further customize a capture session. This section describes the following menu options:

- **Highest layer** — Specifies the highest Expert layer at which Expert analysis will take place.
- **Freeze/Reuse Allocation** — Specifies whether the Expert analyzer should reuse its memory when there is no more room for new network objects.
- **Print Network Objects** — Allows you to print information about a network object to a file or to a printer.
- **Name Width** — Allows you to specify the width (in characters) allotted to names in Expert displays.

Each of these options is described below.

Highest Layer Option

The **Highest layer** option allows you to specify the highest layer at which Expert analysis will take place. For example, if **Highest layer** were set to **Application** (the default), all four Expert layers would be analyzed. However, if **Highest layer** were set to **Network Station**, only the Network Station and DLC Station layers would be analyzed. Because the **Highest layer** option allows you to perform Expert analysis on selected layers only, you can conserve memory and processor time during capture.

Because the amount of traffic on a particular network segment can be huge, the Expert analyzer may sometimes miss some frames. When you need Expert analysis on a very busy network segment, or you know at what layer the problem you are looking for resides, you may want to use the **Highest layer** option.

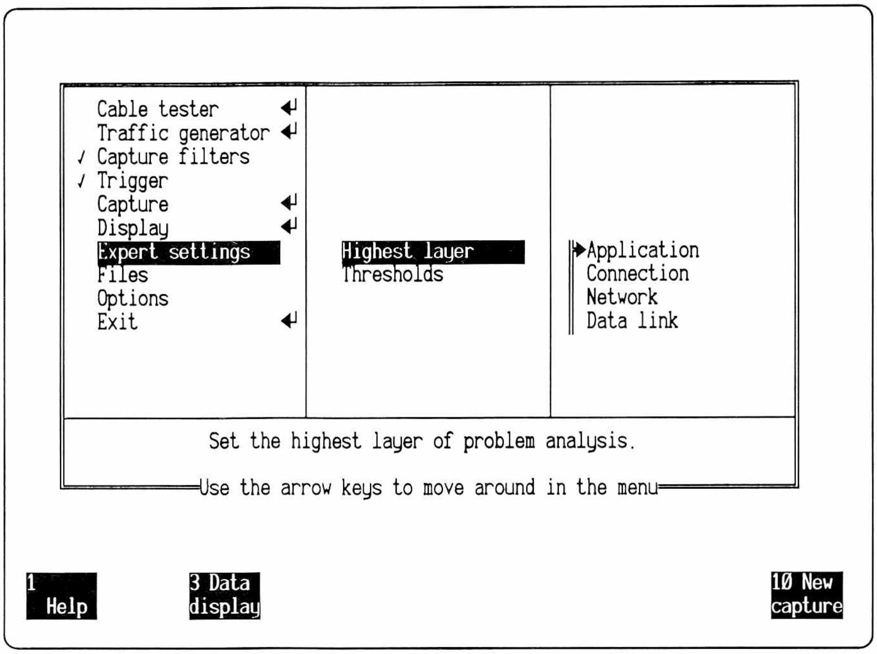
For example, suppose you were concerned with the number of broadcast frames on a very busy network segment. Using the **Highest layer** option, you could specify that the analyzer only perform Expert analysis at the DLC Station layer; the Expert layer concerned with broadcast frames. After capture, when memory and processor time is no longer at a premium, you could reset the **Highest layer** option to **Application**. When you press F3 (**Data display**), the analyzer will reanalyze the frames in the capture buffer for all four Expert layers.

WARNING: When the Expert reanalyzes the frames in the capture buffer, it releases all the network objects it has created, including those gleaned from frames no longer in the capture buffer. The results of post-capture Expert analysis will be based solely on information found in the frames currently in the capture buffer. Once network objects associated with frames outside of the capture buffer have been released, they cannot be regained. See the discussion in "Effects of Changing Expert Thresholds" on page 3–30 for more information on this concept.

To specify the highest Expert layer at which Expert analysis takes place:

1. Move to the **Expert settings\Highest layer** menu.

   Result: The menu in Figure 3–22 appears. Notice that the **Application** layer is currently the highest layer that will receive Expert analysis. That is the default.



Set the highest layer of problem analysis.

Use the arrow keys to move around in the menu

Figure 3–22. Expert settings \ Highest layer menu. Notice that the radio control is set to ***Application****, the default.*

2. Move the highlight to the highest layer at which you want Expert analysis to take place. Press either Enter or Spacebar.

   Result: The radio control moves to the selected layer. All layers below (and including) the selected layer will receive Expert analysis.

Remember that the layers used by the Expert analyzer do not correspond exactly to the OSI model. For a diagram of how the Expert model of network layers maps onto the OSI model, see Figure 3–1 on page 3–5.

Freeze/Reuse Allocation Option

As the Expert analyzer captures frames from the network, it uses the information in those frames to build a database of network objects. Because some networks can be immensely complex in their structure, at some point the Expert analyzer will have no more memory for new network objects in its database. The **Freeze/Reuse Allocation** option allows you to specify what action the analyzer should take when it runs out of memory for new network objects.

The two options are:

- **Freeze allocation** The analyzer will create no more new objects, but will instead continue to interpret network traffic in accordance with the information it has already stored in its database. Symptoms and diagnoses will be revealed according to the information already in the Expert analyzer's database.

- **Reuse allocation** The analyzer will continue to add new objects to its database, overwriting those objects that are least interesting. This is the default. See "How the Expert Analyzer Reuses Network Objects," below.

Depending on the configuration of your unit, the Expert analyzer's database has an upper limit of about 600 network objects.

How the Expert Analyzer Reuses Network Objects

When the Expert analyzer reuses the memory associated with less interesting network objects, it does so via a "smart" algorithm that, in effect, allows it to "forget" outdated network information. The list below summarizes the types of network objects the analyzer will and will not reuse:

The analyzer will not reuse:

- Network objects that have symptoms or diagnoses associated with them
- A network object currently highlighted in the Expert window

The analyzer will reuse:

- Network objects with two or less associated frames and no associated errors

For example, the Expert analyzer will create objects in its database for network stations that have never transmitted or received a frame. Various routing protocols, such as the Routing Information Protocol (RIP), require regular route advertisements showing which stations can be accessed by a given router. The Expert analyzer can learn about non-transmitting stations from such route advertisements. When **Reuse allocation** is selected, the Expert analyzer will reuse objects associated with non-transmitting stations such as these in favor of new information.

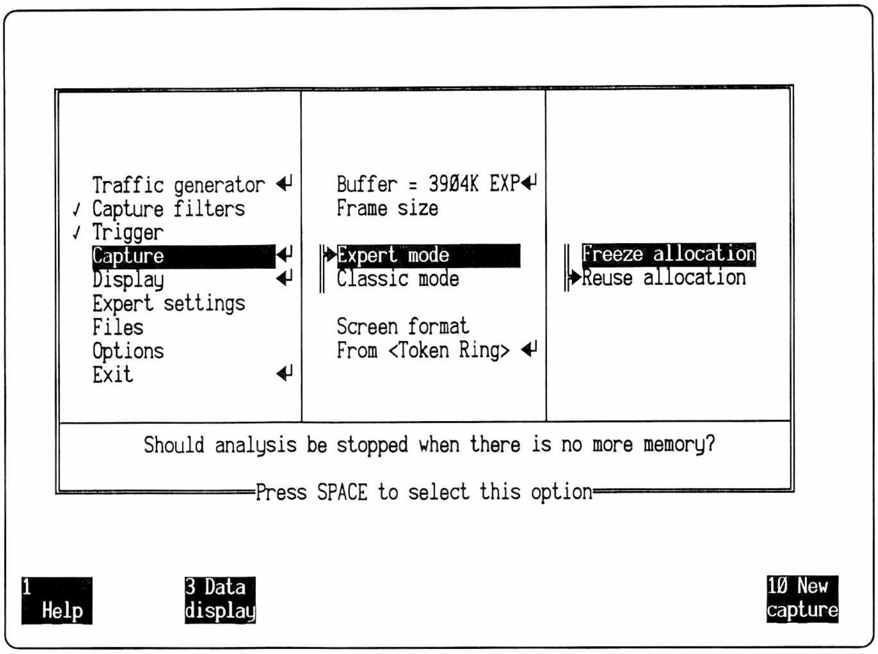
To specify the Expert analyzer's action when memory is exhausted:

1. Use the cursor keys to move to the **Capture\Expert mode** menu.

   Result: A display such as that in Figure 3–23 appears. Notice that currently the radio control points to **Reuse allocation**. That is the default.

2. Use the cursor keys to highlight the desired option, as described above. Press either Enter or Spacebar.

   Result: The radio control moves to the highlighted option. The new option will be effective the next time capture starts.



```
  Traffic generator ↵    Buffer = 39Ø4K EXP↵
✓ Capture filters        Frame size
✓ Trigger
  Capture           ↵   ▸Expert mode           Freeze allocation
  Display           ↵    Classic mode         ▸Reuse allocation
  Expert settings
  Files                  Screen format
  Options                From <Token Ring> ↵
  Exit              ↵

        Should analysis be stopped when there is no more memory?
                    Press SPACE to select this option

1       3 Data                                          1Ø New
 Help   display                                         capture
```

Figure 3–23. Capture \ Expert mode menu.

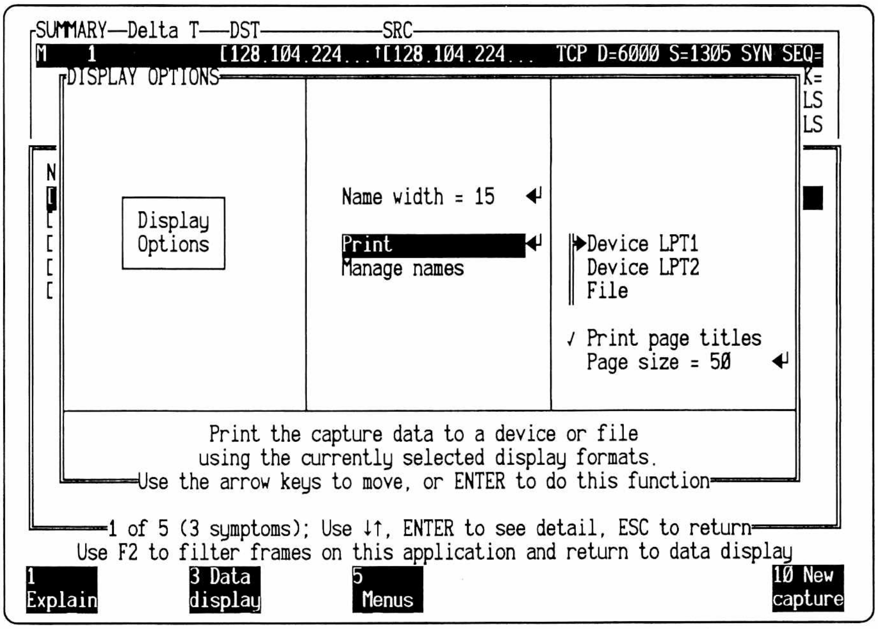
Print Network Objects Option

Just as you can save, print, or import displayed frames, the Expert analyzer also allows you to print information about network objects to a file or printer. This section gives an overview of the options associated with printing reports on network objects. For a complete discussion of the analyzer's printing capabilities, see the *Distributed Sniffer System: Analyzer Operations Manual.*

To prepare for printing a report on a network object, you can define the following options:

- The destination (either a printer or file)
- File format
- Page titles (if any)
- Page size

Figure 3–24 shows the options associated with printing reports on network objects.



```
SUMMARY—Delta T——DST——————SRC——————————————————
M   1        [128.104.224...↑[128.104.224...  TCP D=6000 S=1305 SYN SEQ=
  DISPLAY OPTIONS                                                    K=
                                                                     LS
                                                                     LS
N
[
[           Display       Name width = 15   ↵
[           Options
[                         Print             ↵   ▶Device LPT1
[                         Manage names           Device LPT2
                                                 File

                                               ✓ Print page titles
                                                 Page size = 50     ↵

                   Print the capture data to a device or file
                  using the currently selected display formats.
            Use the arrow keys to move, or ENTER to do this function
      1 of 5 (3 symptoms); Use ↓↑, ENTER to see detail, ESC to return
       Use F2 to filter frames on this application and return to data display
1          3 Data       5                                          10 New
Explain    display      Menus                                      capture
```

Figure 3–24. Menu items associated with printing network objects.

In general, printed reports for network objects combine the information found in the Expert Detail and Statistics windows for a particular object. Printouts of network object information are always preceded by a printout of the Expert Overview. When data is printed, there are no indications of highlighting or color.

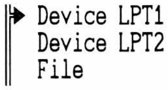
The procedure that follows outlines the steps for printing reports on network objects. For more information about each of the options associated with the **Print** option as it pertains to network objects, see the sections after the procedure.

To create a report on a network object:

1. After capture, display data in the Expert window by pressing F3 (**Data display**).
2. From a display accessible from the Objects/Symptoms column of the Expert window, highlight the object for which you want to create a report. Objects include applications, connections, network stations, and DLC stations.

   Note: You cannot create reports for subnets, global symptoms, or diagnoses.
3. Press F6 (**Disply options**).

   Result: The Display Options menu appears (Figure 3–24).
4. In the Display Options menu, define the destination by moving to the desired option and pressing Spacebar.



```
▶ Device LPT1
  Device LPT2
  File
```

5. Determine whether to include page titles. Move to **Print page titles** and press Spacebar to enable (√) or disable (x) the option.

6. Determine the page size. Move to the **Page size** option and press Enter. In the dialog box that appears, enter a value between 5 and 99 as the desired number of lines per page. The default is 50 lines per page.

7. Move to **Print** and press Enter. Depending on the report destination you specified, the report is either printed on the chosen printer or saved as a file.

   If you chose the **File** option, a dialog box appears. Enter the filename, using no more than eight characters. Do not include an extension; the Sniffer analyzer automatically attaches the extension .PRN to the filename you entered.

Defining the Destination: Printer or File

You can either print displayed data or save it to disk as a file. Figure 3–25 shows a sample report on a network object. In this case, the network object is a connection between the workstation **PamsWorkstation** and the NFS server **MIS-Server**.

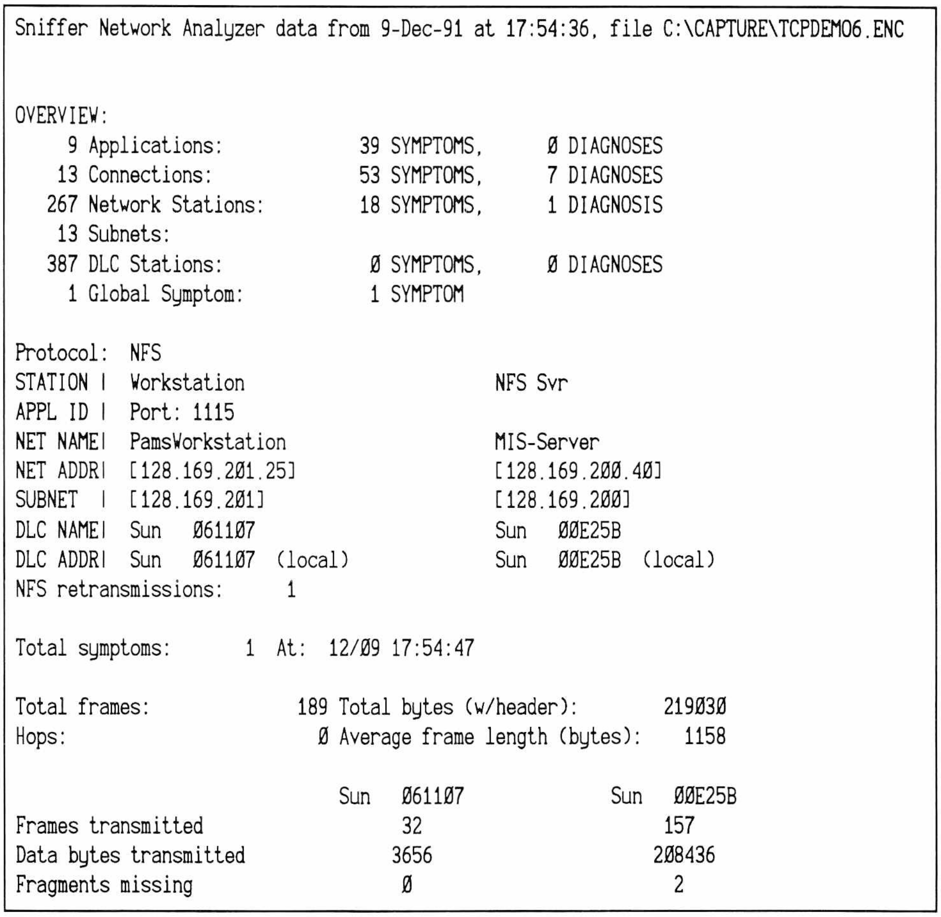
Report destination options include:

LPT1 — A parallel printer attached to the Sniffer Server's LPT1 port.

LPT2 — A printer attached to the SniffMaster Console from which you are operating the Server. (The Console may then redirect the output to a file on its own hard disk, if it has been configured to do so.) For a discussion of Console configurations, see the *Distributed Sniffer System: Console Installation and Operations Manual.*

File — A file that is saved to the Sniffer Server's hard disk.

For more details on the physical setup of attached printers, see the *Distributed Sniffer System: Console Installation and Operations Manual.*



Printed reports on network objects always include the Expert Overview.

Information from Detail window for this network object.

Information from Statistics window for this network object.

```
Sniffer Network Analyzer data from 9-Dec-91 at 17:54:36, file C:\CAPTURE\TCPDEMO6.ENC


OVERVIEW:
     9 Applications:             39 SYMPTOMS,      Ø DIAGNOSES
    13 Connections:              53 SYMPTOMS,      7 DIAGNOSES
   267 Network Stations:         18 SYMPTOMS,      1 DIAGNOSIS
    13 Subnets:
   387 DLC Stations:              Ø SYMPTOMS,      Ø DIAGNOSES
     1 Global Symptom:            1 SYMPTOM

Protocol:  NFS
STATION |  Workstation                  NFS Svr
APPL ID |  Port: 1115
NET NAME|  PamsWorkstation              MIS-Server
NET ADDR|  [128.169.2Ø1.25]             [128.169.2ØØ.4Ø]
SUBNET  |  [128.169.2Ø1]                [128.169.2ØØ]
DLC NAME|  Sun   Ø611Ø7                 Sun   ØØE25B
DLC ADDR|  Sun   Ø611Ø7  (local)        Sun   ØØE25B  (local)
NFS retransmissions:     1

Total symptoms:      1  At:  12/Ø9 17:54:47

Total frames:             189 Total bytes (w/header):       219Ø3Ø
Hops:                       Ø Average frame length (bytes):   1158

                              Sun   Ø611Ø7           Sun   ØØE25B
Frames transmitted                32                      157
Data bytes transmitted          3656                   2Ø8436
Fragments missing                  Ø                        2
```

Figure 3–25. Printed report on a network object.

Choosing Page Titles

You can choose whether to include page titles for each page. Page titles specify the date and time the data was recorded, the network name (for a "live" capture) or the name of the file (for a capture from a file), and the page number. There are two blank lines between the heading and the start of the data.

If you enable the **Print page titles** option, you also cause explicit page breaks because the Sniffer analyzer includes a form-feed character after the last non-blank line of each page.

Choosing Page Size

You can also set the page size, which determines the number of lines per page. The default is 50 lines. Depending on whether you enabled the **Print page titles** option, this setting would result in either 50 printed lines or, with a page title, two blank lines and 47 lines of data. Since each page break is indicated by an explicit form feed, there is no separate setting for the physical length of the paper.

Name Width Display Option

You can define the width of the name field in the Expert summary and detail displays, from 6 characters up to 31 characters (the default is 15 characters). For example, if the Expert analyzer discovers many large names, you may want to make the name field wider to accommodate the names.

Once you've increased the name width, other information fields may be partially hidden beyond the right limit of the display. That information is still there; you simply need to scroll to reach it. The Expert analyzer allows you to use the cursor keys to scroll horizontally and read information temporarily "hidden" at the edge of the display.

If the display includes a name longer than the specified name width, the Sniffer analyzer truncates that name and replaces its last two visible characters with dots (to show that the name has been truncated). For example, if the **Name width** option specifies an 8-character field and the analyzer discovers the 10-character name "**FileServer**," the Summary view would show "**FileSe. .** "

To define the Name width option:

1. Move to **Name width=** and press Enter.

   The **Name width** command is available in three places in the Sniffer analyzer menus:
   - In the **Capture\Screen Format\Expert window** menu.
   - In the **Display** menu.
   - From the **Display Options** menu. The **Display Options** menu is available by pressing F6 (**Disply options**) during post-capture display.

   All three locations are linked. If you change the name width in one location, it is automatically synchronized throughout the menus.

2. In the dialog box that appears, enter the desired name width.

   Note: The width you specify in this dialog box will apply to both the Expert and Classic summary and detail displays.

How the Expert Analyzer Learns Symbolic Names

During capture, the Expert analyzer uses its real-time protocol interpreters to learn about the symbolic names for the various network stations, servers, routers, and other network stations. The Expert analyzer can rapidly decode the frames it captures, associating the symbolic names it finds with the related network stations. As the analyzer learns names, it will substitute the symbolic names for the hex, IP, or DECnet addresses in the Expert displays.

Some network protocols have a command that lists all users currently logged on to a given file server. When this occurs, the Expert analyzer captures the relevant packets and extracts all the names from that packet, associating them with the appropriate network address. The following procedure shows how to use this "trick" to help the analyzer learn names almost instantly.

To help the Expert analyzer learn symbolic names:

1. From a workstation "visible" by the Sniffer Network Analyzer, type the following command:

   -If Novell:

   ```
   USERLIST /A
   ```

   -If DECnet

   ```
   SHOW KNOWN NODES
   ```

   -If TCP/IP running Sun Network Information Services™ (also known as Sun Yellow Pages).

   ```
   YPCAT HOSTS.BYNAME
   ```

2. Once the Expert analyzer captures the relevant packets, it will substitute the symbolic names it has learned for the addresses in the Expert displays.
3. At the end of the capture session, you may want to use the **Save names** option to save all of the names the Expert analyzer has learned to the name table. For more information on the **Save names** option and how the analyzer works with the name table, see the *Distributed Sniffer System: Analyzer Operations Manual.*

Note: The Expert analyzer still "knows" the actual address of each station. That information is available in the Detail window. See the next chapter for more information on the Detail window.

Note: In a Novell environment, this trick only works for those stations which are currently logged on to the file server to which the request is made. For example, if WorkStation A is logged on to the file server BIZ-ONE and makes a `USERLIST /A` request, the analyzer will only learn the symbolic names of those stations currently logged on to BIZ-ONE.

Note: Two Console alarms generated by the same diagnosis will display different station names in the text description field if the symbolic name was identified between the sending of the two alarms.

CHAPTER FOUR: EXPERT ANALYZER CAPTURE AND DISPLAY 4

Expert Analyzer Capture and Display

Overview

You can display the results of Expert analysis at many different levels of detail. This chapter describes the various displays containing the results of Expert analysis. The chapter is organized as follows:

- How to navigate through the Expert displays.
- Description of the Global Statistics display
- Descriptions of the various Diagnosis displays. Each Diagnosis detail display is described.
- Descriptions of the various Symptom and Network Object displays.

The chapter also discusses traversing the various Expert displays to get the maximum amount of information on a network problem or connection.

All the Expert screen displays available during capture are also available during post-capture display. You can navigate through the Expert window during display just as you would during capture. The instructions and descriptions in this chapter are unique to neither capture nor display but only to the Expert window.

Displaying Analysis Results In the Expert Window

When you start capture in Expert mode, the analyzer automatically sets the screen format to the Expert window. By default, the analyzer displays the Expert Overview. The Expert Overview provides your "home base" for tracking and investigating network problems detected by the analyzer. The Expert Overview tabulates all detected network objects, symptoms, and diagnoses, organizing them by the Expert layer at which they occur. You can use the cursor keys to highlight the various fields in the Expert Overview and press Enter to view more detailed screens.

For definitions of, "network objects," "symptoms," and, "diagnoses," see the sections beginning on page 2–3.

Figure 4–1 summarizes the various displays available in the Expert window.

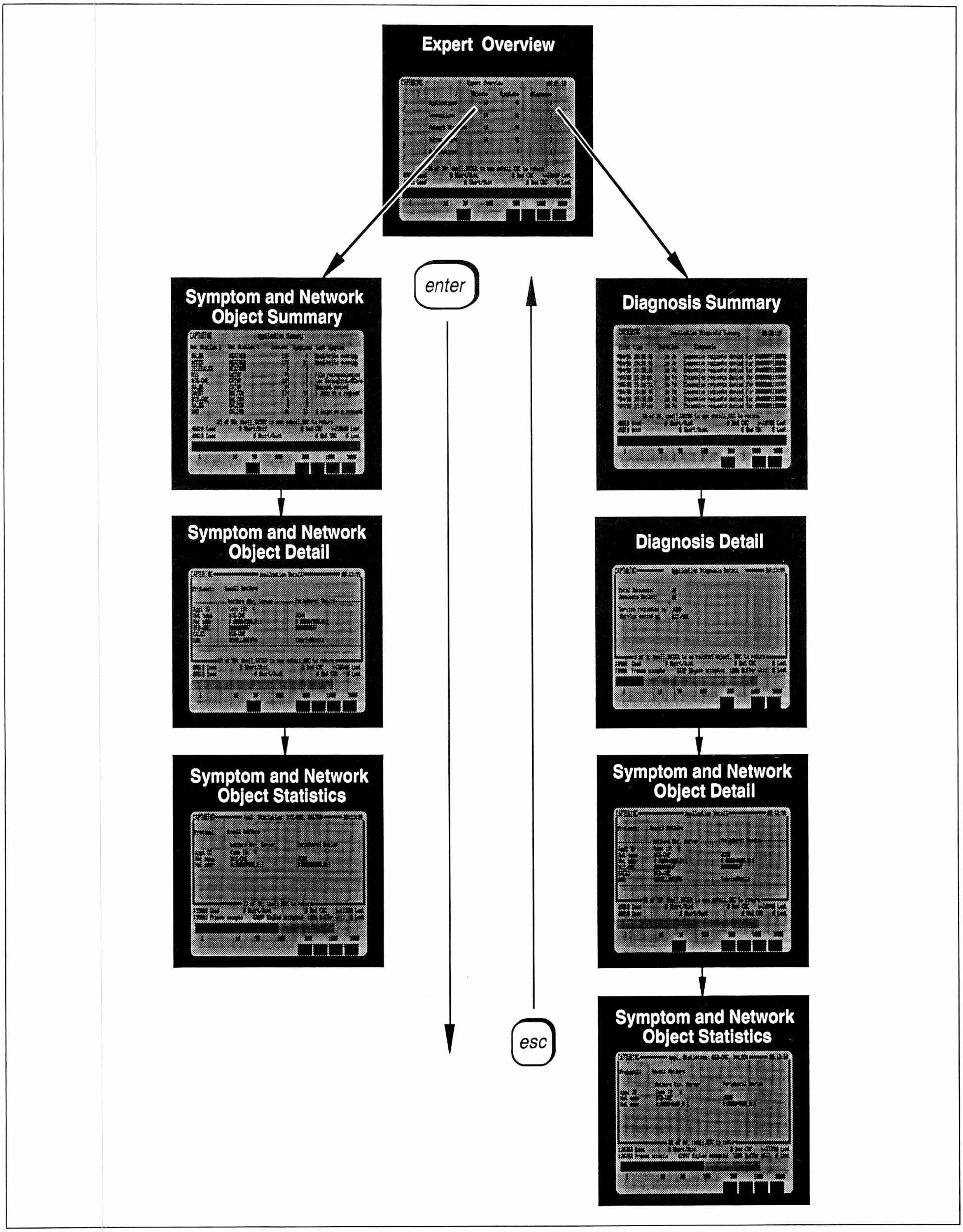

Expert Overview
Symptom and Network Object Summary
enter
Diagnosis Summary
Symptom and Network Object Detail
Diagnosis Detail
Symptom and Network Object Statistics
Symptom and Network Object Detail
esc
Symptom and Network Object Statistics

Figure 4–1. Schematic of the various Expert windows.

Figure 4–1 introduces an important concept for working with the Expert analyzer. Note that while the Expert displays begin with the Expert Overview, subsequent displays are divided between two categories:

- Diagnosis-related displays
- Symptom and Network Object-related displays

Although the various displays in these two categories are similar in content, their purposes are different. The diagnosis-related displays allow you to track network problems that demand immediate attention. The symptom and network object displays provide you with a barometer of the overall health of your network. Typically, the quantity of symptoms on a given network will greatly exceed the number of diagnoses.

Expert analysis results can be displayed at four levels of detail– overview, Summary, detail, or statistics displays. The list that follows briefly describes the contents of each display.

Overview

The Expert Overview provides a summary of all information detected by the Expert analyzer. The Expert Overview tabulates the number of network objects, symptoms, and diagnoses detected at each Expert layer, in addition to a one-line summary of some critical diagnoses.

It may be helpful to think of the Expert Overview as a "home base" from which you can traverse out to the various Expert analyzer submenus. By highlighting the various fields in the Expert Overview and pressing Enter, you can receive more detailed information about specific network problems detected by the Expert analyzer.

Summary

The Diagnosis Summary window contains a list of all diagnoses detected at the selected layer. This list contains brief descriptions of the detected diagnoses and when they occurred.

Symptom and Network Object Summary windows list all network objects detected at the selected layer and a one-line description of the last symptom (if any) associated with each network object. Summary windows are described starting on page 4–36.

Detail

Diagnosis Detail displays show specific information about a particular diagnosis. The information in this view is designed to help you solve the network problem indicated by the diagnosis. Information in this display could include the addresses of the most active stations during a traffic burst, the address of a slow server, or the name of a non-responsive station. The exact information depends on the particular diagnosis. The various Diagnosis Detail displays are described starting on page 4–13

Symptom and Network Object Detail windows show detailed information about the highlighted network object and any symptoms associated with that object. This information could include the addresses of all stations connected to a selected server, the average packet length of frames on a particular connection, and so on. The exact information depends on the Expert layer and the highlighted network object. Symptom and Network Object Detail windows are described starting on page 4–47.

Statistics

Statistics displays provide specific information about a particular connection or network station. The information in this view could include total bytes transferred on a connection, average frame length, average file performance and number of broadcast frames sent. The exact information depends on the Expert layer selected. Statistics displays are described starting on page 4–54.

In addition to these views, there is also a Global Statistics view. The Global Statistics view provides a percentage breakdown by protocol family of all detected network traffic. Additionally, the Global Statistics view provides information on bandwidth utilization and general information about the current capture session. The Global Statistics window is described starting on page 4–64.

Each of these displays is described further in later sections.

Navigating the Expert Window

You can always navigate among the various Expert displays using these methods:

- To move from a general to specific display, highlight a field that interests you and press Enter. (Use Cursor Up, Cursor Down, PgUp, PgDn, Home, and End to move the highlight.) For example, in the Expert Overview, you can highlight the Diagnoses field at the Application layer and press Enter to display a list of diagnoses detected at the Application layer.
- To move from a specific to a general display, press Esc.

- If the width allotted to names in the Expert displays has been expanded with the **Name width** command, there may be some information out of sight at the right edge of the Summary displays. The analyzer will indicate this by replacing the last two visible characters with periods. (For example, "Fileserver" might become "Fileserv..")You can use the cursor keys to scroll horizontally until the hidden information becomes visible. Horizontal scrolling is available only in the Expert Summary displays (and in the Classic display window). For more information on the **Name width** command, see "Name Width Display Option" on page 3–51.
- There are also several function keys which can speed your navigation through the Expert Overview. These keys are described in "Advanced Navigation Techniques" on page 4–77.

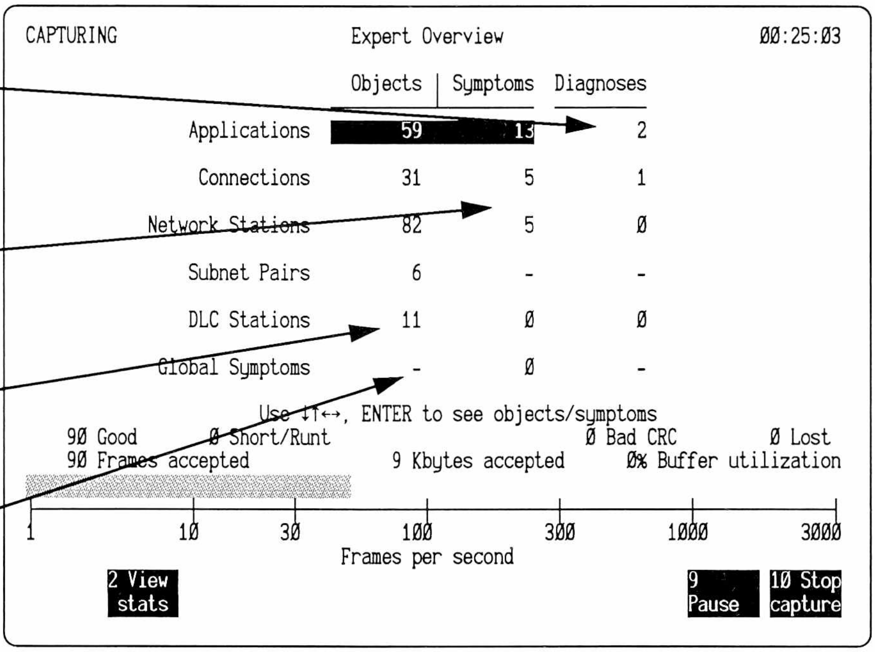
Explain messages are available at each level of display. However, capture must be paused before pressing F1 (**Explain**) to invoke these messages. Explain messages are context-sensitive; their contents change according to the information being displayed. To terminate the display of an Explain screen, press Esc. You can display as many explain messages as you want while capture is paused. Simply switch to another display or highlight a different field in the current display and press F1 to invoke the message for that topic.

Note: During post-capture Display routines, Explain messages are always available in the Expert window by pressing F1 (**Explain**).

The best way to learn how to navigate through the Expert displays is to experiment with your analyzer, navigating through the various windows.

The Expert Overview Display

When you start capture in Expert mode, the Expert Overview appears (Figure 4–2). The Expert Overview provides a summary of network activity at each Expert layer. There are separate counters for the number of network objects, symptoms, and diagnoses detected at each Expert layer, allowing you to maintain a constant overview on the health of your network.



```
CAPTURING                     Expert Overview                         ØØ:25:Ø3

                              Objects | Symptoms  Diagnoses

             Applications          59        13          2
              Connections          31         5          1
         Network Stations          82         5          Ø
             Subnet Pairs           6         -          -
             DLC Stations          11         Ø          Ø
           Global Symptoms          -         Ø          -

                     Use ↓↑←→, ENTER to see objects/symptoms
  9Ø Good          Ø Short/Runt                  Ø Bad CRC         Ø Lost
  9Ø Frames accepted           9 Kbytes accepted        Ø% Buffer utilization

1             1Ø      3Ø        1ØØ         3ØØ        1ØØØ        3ØØØ
                            Frames per second
     2 View                                                   9       1Ø Stop
     stats                                                    Pause   capture
```

Number of diagnoses detected at each Expert layer

Number of symptoms detected at each Expert layer

Number of network objects detected at each Expert layer

Hyphens indicate that counts are not applicable– not that the count is zero.

Figure 4–2. The Expert Overview.

The Expert Overview is organized as a table with six rows and three columns. The rows represent the four Expert layers, plus one row for subnet pairs and one row for global symptoms. Subnet Pairs and Global Symptoms are not Expert layers. The purpose of these fields is to provide more information about subnets and global symptoms, such as traffic bursts.

The three columns include:

- **Objects** - the number of network objects detected at this Expert layer (that is, the number of connections at the Application layer, connections at the Connection layer, Network Stations, and DLC Stations detected since capture started).
- **Symptoms** - the number of symptoms detected at this Expert layer.
- **Diagnoses** - the number of diagnoses detected at this Expert layer.

For definitions of network objects, symptoms, and diagnoses, see "Expert Analyzer Terminology" on page 2–3.

Navigating through the Expert Overview

Each cell within the Expert Overview table is a gateway to more detailed subscreens. By using the cursor keys to highlight a particular field and pressing Enter, you can see more detailed information about the objects, symptoms, and diagnoses at the highlighted layer. These subdisplays are described in later sections.

Note: While Objects and Symptoms are tabulated separately, you cannot view them separately, because their displays are integrated. The cursor indicates this by highlighting both columns, as in Figure 4–2.

Note: The analyzer has an upper limit of 100 diagnoses. While it is unlikely that you would ever reach this point (unless thresholds were set artificially low), the analyzer can record no more than 100 diagnoses during a given capture session. If this is a problem, you may want to set the Expert thresholds higher (see "Setting Thresholds for Symptoms and Diagnoses" on page 3–13), consider setting a capture filter, or change **Highest layer** to a lower Expert layer (see "Highest Layer Option" on page 3–44).

Other Counters in the Expert Overview

The Expert Overview shows the same statistics near the bottom of the screen as any capture display. For example, it includes the number of frames captured, the percentage of network usage, buffer utilization, and so on, which you would also see on an analyzer capturing in Classic mode. The exact format depends on the options you select in the **Capture\Screen format** menu. For more information on these counters, see the *Distributed Sniffer System: Analyzer Operations Manual.*

Diagnosis-Related Displays

This section describes the various displays accessible from the **Diagnoses** column of the Expert Overview. The Expert displays accessible from the **Objects/Symptoms** column of the Expert Overview are described starting on page 4–36. Note that the same displays are available in the Expert window regardless of whether the analyzer is capturing or displaying frames.

You may want to refer to Figure 4–1 on page 4–4 for a schematic of the various Expert windows and how they relate to one another.

Diagnosis Summary Window

The Diagnosis Summary window lists all diagnoses generated by the Expert analyzer at the selected Expert layer. The analyzer updates the appropriate diagnosis count in the Expert Overview each time it makes a diagnosis. Each diagnosis is a conclusion that the analyzer makes when predefined thresholds have been exceeded. The procedure below explains how to display a Diagnosis Summary window.

To display a Diagnosis Summary window:

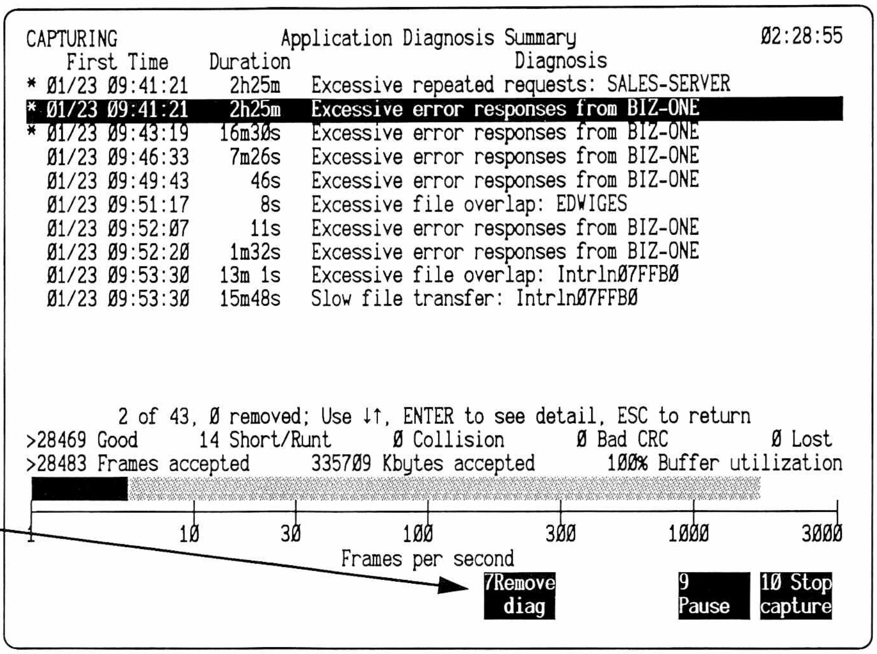
1. In the Expert Overview, use the cursor keys to highlight a particular layer in the Diagnoses column that shows at least one diagnosis. Press Enter.

   Result: The Diagnosis Summary window appears, as shown in Figure 4–3.

   Note: The Summary window appears only if diagnoses exist at the selected layer.

Each diagnosis in the Summary window represents an important "clue" that might lead to the discovery of a network problem.

You can temporarily remove a diagnosis from display. See page 4–12 for more information on removing diagnoses.



```
CAPTURING                 Application Diagnosis Summary                    Ø2:28:55
    First Time     Duration                   Diagnosis
* Ø1/23 Ø9:41:21     2h25m   Excessive repeated requests: SALES-SERVER
* Ø1/23 Ø9:41:21     2h25m   Excessive error responses from BIZ-ONE
* Ø1/23 Ø9:43:19    16m3Øs   Excessive error responses from BIZ-ONE
  Ø1/23 Ø9:46:33     7m26s   Excessive error responses from BIZ-ONE
  Ø1/23 Ø9:49:43       46s   Excessive error responses from BIZ-ONE
  Ø1/23 Ø9:51:17        8s   Excessive file overlap: EDWIGES
  Ø1/23 Ø9:52:Ø7       11s   Excessive error responses from BIZ-ONE
  Ø1/23 Ø9:52:2Ø     1m32s   Excessive error responses from BIZ-ONE
  Ø1/23 Ø9:53:3Ø    13m 1s   Excessive file overlap: IntrlnØ7FFBØ
  Ø1/23 Ø9:53:3Ø    15m48s   Slow file transfer: IntrlnØ7FFBØ


         2 of 43, Ø removed; Use ↓↑, ENTER to see detail, ESC to return
>28469 Good      14 Short/Runt      Ø Collision        Ø Bad CRC          Ø Lost
>28483 Frames accepted       3357Ø9 Kbytes accepted      1ØØ% Buffer utilization
```

Figure 4–3. Diagnosis Summary window; in this case, at the Application layer.

The following list describes the three types of information shown in the Summary display:

First Time — The time when the analyzer first makes the diagnosis.

Duration — The length of time during which the diagnosis is valid. Suppose the diagnosis is **Excessive error responses from BIZ-ONE**, as in Figure 4–3. This means that the ratio of denied application requests to successful requests has exceeded the **Error resp** threshold in the Expert settings\Thresholds menu. This condition has been active for a total of two hours and 25 minutes.

An asterisk in the first column indicates that the diagnosis is still active. In the above example, it means that BIZ-ONE is currently denying excessive application requests. The asterisk disappears and the counter for duration stops incrementing when the percentage of denied requests drops below the **Error resp** threshold. If the diagnosis condition begins again, the analyzer will increment the existing counter cumulatively. The duration counter does not imply consecutive time.

Diagnosis — A statement describing a potential network problem. It may or may not be a valid conclusion. Before making a final judgment, you might want to take into account circumstances that are not known to the analyzer.

You should press F1 to display the Explain message related to the highlighted diagnosis. The Explain message reminds you of the thresholds that affect the diagnosis and includes suggestions on how to examine other statistics to assess the seriousness of the problem. To return to the Summary display, press Esc.

Temporarily Removing Diagnoses From the Expert Window

During your investigation of network problems, you may want to limit the diagnostic displays in the Expert window to only those problems which currently concern you. The procedure below explains how to temporarily remove a diagnosis from the Expert window.

To temporarily remove a diagnosis from the Expert window:

1. Use the cursor keys to display one of the following:
   - A Diagnosis Summary window
   - A Diagnosis Detail window
2. Highlight the diagnosis which you want to temporarily remove from the display.
3. Notice the dynamic function key label at the bottom of the display for F7 (**Remove diag**). Figure 4–3 shows the label.

   Press F7 (**Remove diag**) to temporarily remove the highlighted diagnosis from display.

You can remove as many diagnoses as you like, narrowing the display to show only those that concern you. The removed diagnoses have not been erased; they have simply been removed from display. The procedure below explains how to restore them.

To restore removed diagnoses to the display:

1. Use the cursor keys to display one of the following:
   - A Diagnosis Summary window
   - A Diagnosis Detail window
2. If there are diagnoses that have been removed, and can now be restored, the function key label F8 (**Restore diags**) appears. Press F8 to restore the removed diagnoses.

Note: You cannot restore diagnoses individually. Pressing F8 restores all diagnoses removed during the current Expert session.

Note: Diagnoses that have been removed are not used in determining the overall Server alarm level reported to the Console.

Diagnosis Detail Displays

Diagnosis Detail displays provide information important to the investigation of a network problem. The exact information in the Detail display depends on the nature of the highlighted diagnosis. For example, the Detail display for the **Slow server** diagnosis lists the addresses of all stations that received a slow response from a given server. This section describes the Detail display for each diagnosis made by the Expert analyzer. The procedure below explains how to view a Diagnosis detail display.

To display a Diagnosis Detail window:

1. In the Expert Overview, use the cursor keys to highlight a particular layer in the Diagnoses column that shows at least one diagnosis. Press Enter.

   Result: The Diagnosis Summary window appears.

2. In the Summary window, use the cursor keys to highlight the diagnosis you want to investigate. Press Enter.

   Result: The Diagnosis Detail display for the selected diagnosis appears.

Figure 4–4 summarizes the Diagnosis Detail displays and their related Expert thresholds. The displays are organized in alphabetical order.

Diagnosis	Detail Window shown on:	Related Expert Threshold	Threshold described on:
Broadcast Storm	page 4–15	Broadcast Diagnosis	page 3–25
Duplicate Network Address	page 4–16	Duplicate Address Percentage	page 3–23
Excessive Repeated Requests	page 4–17	Filter Time/Loop %	page 3–18
Excessive Requests Denied	page 4–18	Denied Request %	page 3–19
File Overlap/Retransmission	page 4–19	Slow File %	page 3–20
High Rate of Congestion	page 4–20	Receiver Congestion	page 3–26
High Rate of Line/Burst Errors	page 4–21	Ring Errors	page 3–27
High Rate of Physical Errors	page 4–22	Physical Errors	page 3–25
High Rate of Remove from Ring Reqs	page 4–23	Station Removed	page 3–27
High Rate of Ring Entries	page 4–24	Ring Entries	page 3–26
High Rate of Ring Purges	page 4–25	Ring Purge Diagnosis	page 3–27
LAN Overloaded	page 4–26	LAN Overload / LAN Overload % WAN Overload / Overload Timer	page 3–24 page 3–28
Local Router	page 4–27	No threshold	
Multiple Routers to Station	page 4–28	Multiple Routers	page 3–22
Non-responsive Station	page 4–29	No responses	page 3–21
Retransmissions	page 4–31	Retransmission %	page 3–21
Ring beaconing	page 4–32	No threshold	
Slow File Transfer	page 4–33	Slow File %	page 3–20
Slow Server	page 4–34	Response Time/Slow Response %	page 3–17
Underloaded Network	page 4–35	WAN Underload/Underload Timer	page 3–28

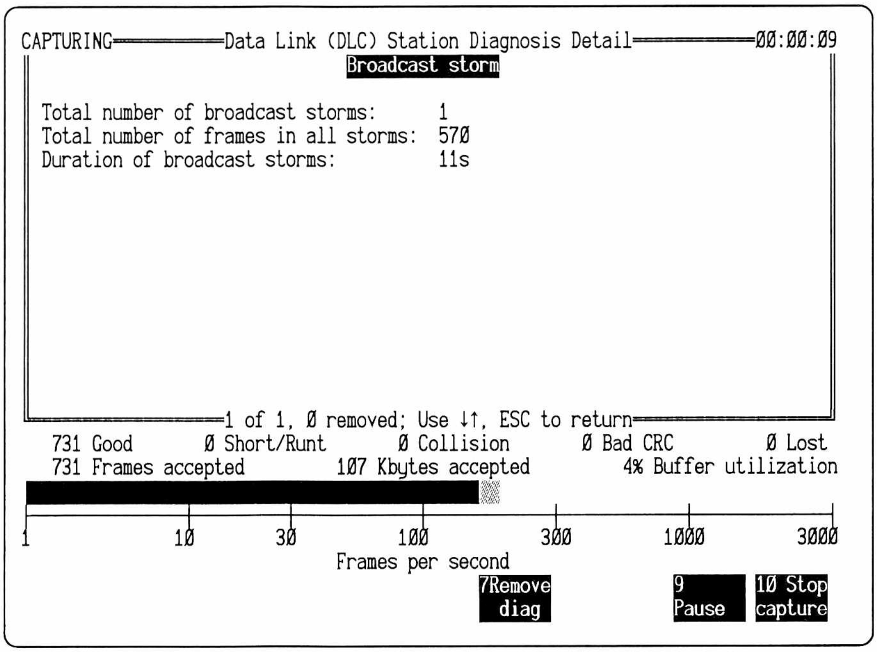
Figure 4–4. Diagnosis Detail displays and their related Expert thresholds.

Broadcast Storm

The analyzer diagnoses a broadcast storm condition when the number of broadcast frames per second exceeds the threshold specified by **Broadcast dg** in the **Expert Settings** menu. For more information on the **Broadcast dg** threshold, see page 3–25.

The detail display, shown in Figure 4–5, provides the following information:

- **Total number of broadcast storms.** Number of broadcast storm diagnoses made by the analyzer during this capture session. When the number of broadcast frames per second falls below the **Broadcast dg** threshold, the current broadcast storm is considered to be finished. If the threshold is exceeded again, a new broadcast storm diagnosis will be generated.
- **Total number of frames in all storms.** Total number of frames associated with all broadcast storms currently diagnosed by the analyzer.
- **Duration of broadcast storms.** Total length (in seconds) of all broadcast storms currently diagnosed by the analyzer.



```
CAPTURING═══════Data Link (DLC) Station Diagnosis Detail════════ØØ:ØØ:Ø9
                            Broadcast storm

 Total number of broadcast storms:      1
 Total number of frames in all storms:  57Ø
 Duration of broadcast storms:          11s

═════════════1 of 1, Ø removed; Use ↓↑, ESC to return═══════════════
 731 Good        Ø Short/Runt      Ø Collision      Ø Bad CRC       Ø Lost
 731 Frames accepted       1Ø7 Kbytes accepted        4% Buffer utilization
```

Figure 4–5. Detail display for the diagnosis, "Broadcast storm."

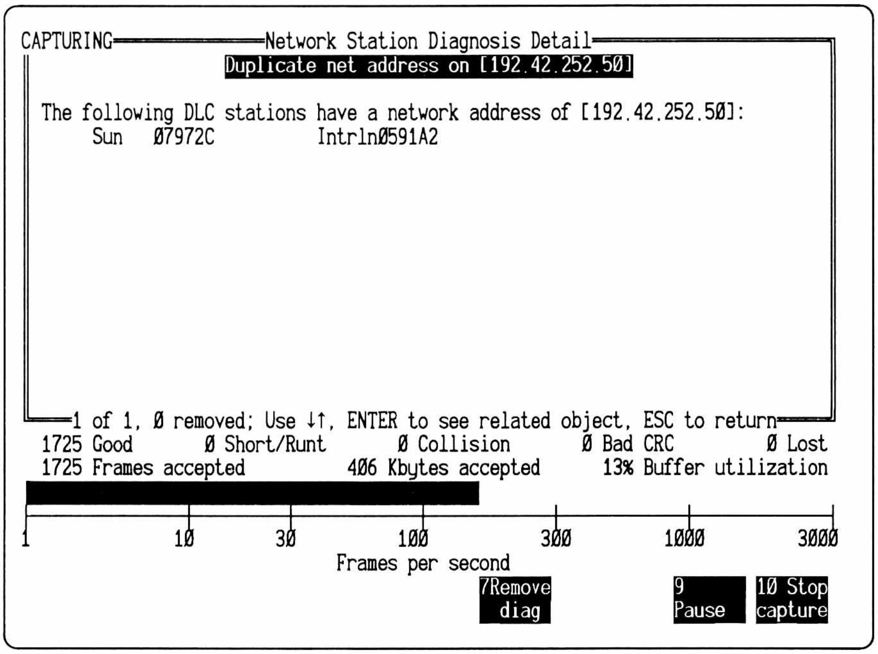
Duplicate Network Address

The analyzer generates the **Duplicate net address** diagnosis when two or more DLC stations are associated with the same network address. In a DECnet environment, the **Duplicate Address percentage** threshold can be used to fine-tune this diagnosis. For more information on the **Duplicate Address percentage** threshold, see page 3–23.

The detail display for the **Duplicate net address** diagnosis provides the following information:

Network address	The network address associated with more than one DLC station.
DLC stations	The addresses of all DLC stations associated with the duplicate network address.

Figure 4–6 shows a typical detail display for the **Duplicate net address** diagnosis. In this example, the network address [192.42.252.50] is associated with both the DLC stations Sun 07972C and Intrln0591A2.



```
CAPTURING══════════════Network Station Diagnosis Detail═══════════════════════
                       Duplicate net address on [192.42.252.5Ø]

 The following DLC stations have a network address of [192.42.252.5Ø]:
      Sun   Ø7972C          IntrlnØ591A2

═══1 of 1, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═══
 1725 Good        Ø Short/Runt       Ø Collision      Ø Bad CRC       Ø Lost
 1725 Frames accepted          4Ø6 Kbytes accepted     13% Buffer utilization
```

Figure 4–6. Detail display for the diagnosis, "Duplicate net address."

Excessive Repeated Requests

The analyzer generates the **Excessive repeated requests** diagnosis when the number of loops on a given connection exceeds the **Loop %** threshold of total application requests. For more information on the **Loop %** threshold and how the analyzer recognizes loop packets, see the sections “"Filter Time",” and “"Loop Percentage",” starting on page 3–18.

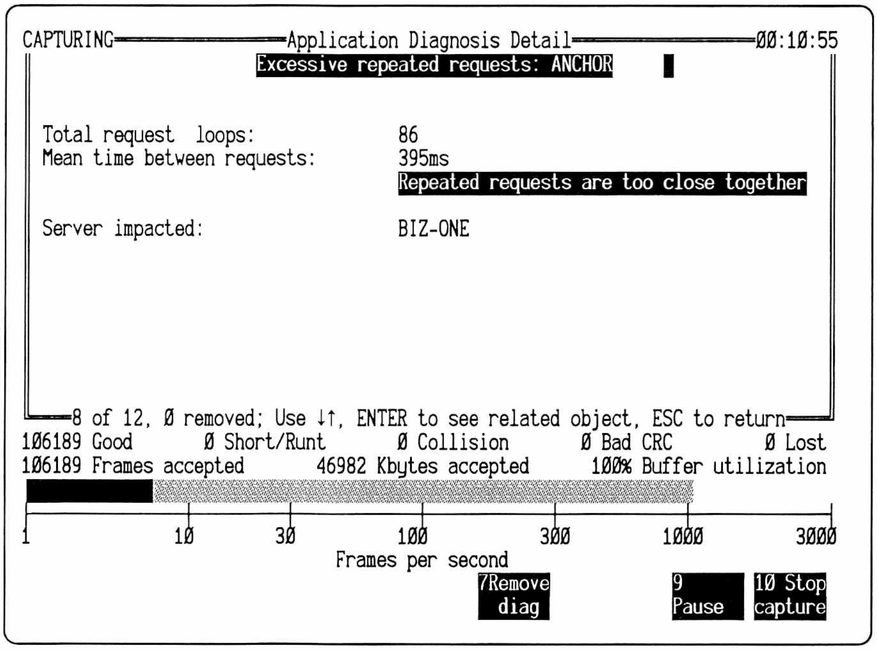
The detail display for **Excessive repeated requests** provides the following information:

Total requests loops — The total number of repeated requests sent out by this station. The requests can be of different types.

Mean time between requests — The total amount of time a station sends repeated requests divided by the total number of repeated requests.

Server impacted — Server impacted is the server to which this station sends the repeated requests.

Figure 4–7 shows a typical detail display for the Excessive repeated requests. In this example, the station ANCHOR has sent excessive repeated requests to the server BIZ-ONE.



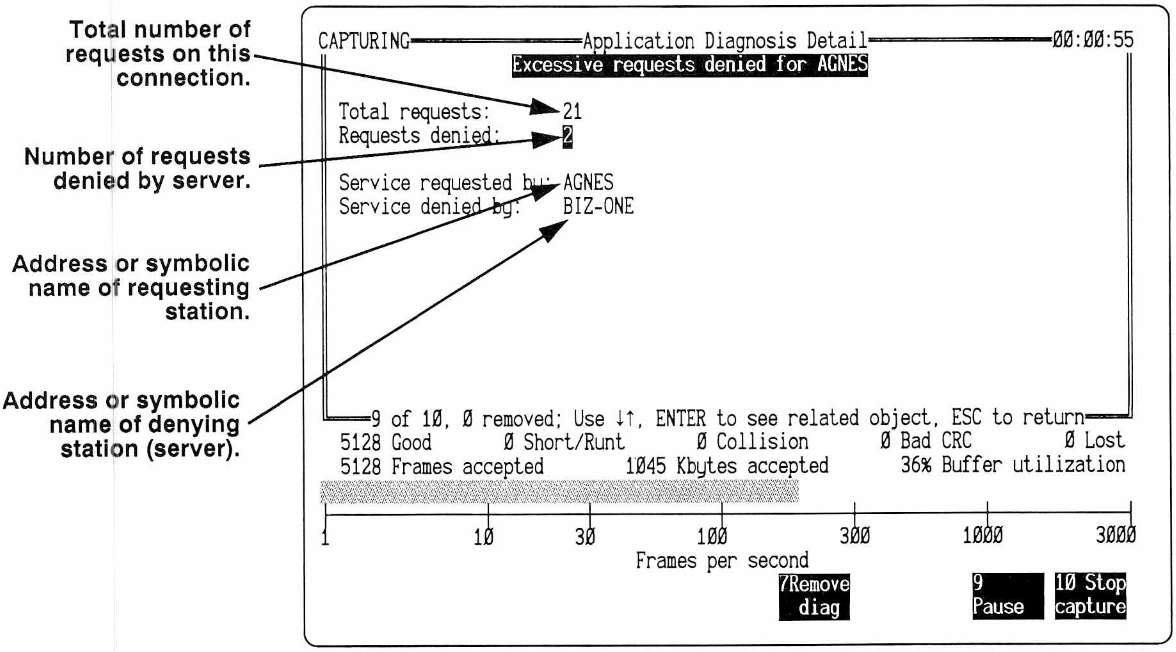
```
CAPTURING══════════════Application Diagnosis Detail══════════════ØØ:1Ø:55
                        Excessive repeated requests: ANCHOR

 Total request  loops:              86
 Mean time between requests:        395ms
                                    Repeated requests are too close together

 Server impacted:                   BIZ-ONE

═══8 of 12, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═══
1Ø6189 Good       Ø Short/Runt       Ø Collision       Ø Bad CRC       Ø Lost
1Ø6189 Frames accepted     46982 Kbytes accepted     1ØØ% Buffer utilization
```

Figure 4–7. Detail display for the diagnosis, “Excessive repeated requests.”

Excessive Requests Denied

The analyzer generates the diagnosis **Excessive requests denied** when the percentage of denied versus successful application requests exceeds the **Denied request** % threshold in the **Expert settings** menu. For more information on this threshold, see page 3–19.

The information provided by the detail display for this diagnosis is described at the left of Figure 4–8.



Total number of requests on this connection.

Number of requests denied by server.

Address or symbolic name of requesting station.

Address or symbolic name of denying station (server).

```
CAPTURING═══════════Application Diagnosis Detail══════════════ØØ:ØØ:55
                  Excessive requests denied for AGNES

 Total requests:       21
 Requests denied:      2

 Service requested by: AGNES
 Service denied by:    BIZ-ONE

═══9 of 1Ø, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═══
 5128 Good       Ø Short/Runt       Ø Collision       Ø Bad CRC        Ø Lost
 5128 Frames accepted       1Ø45 Kbytes accepted       36% Buffer utilization

 1         1Ø       3Ø        1ØØ        3ØØ        1ØØØ        3ØØØ
                          Frames per second
                                      7Remove        9       1Ø Stop
                                       diag        Pause     capture
```

Figure 4–8. Detail display for the diagnosis, "Excessive requests denied."

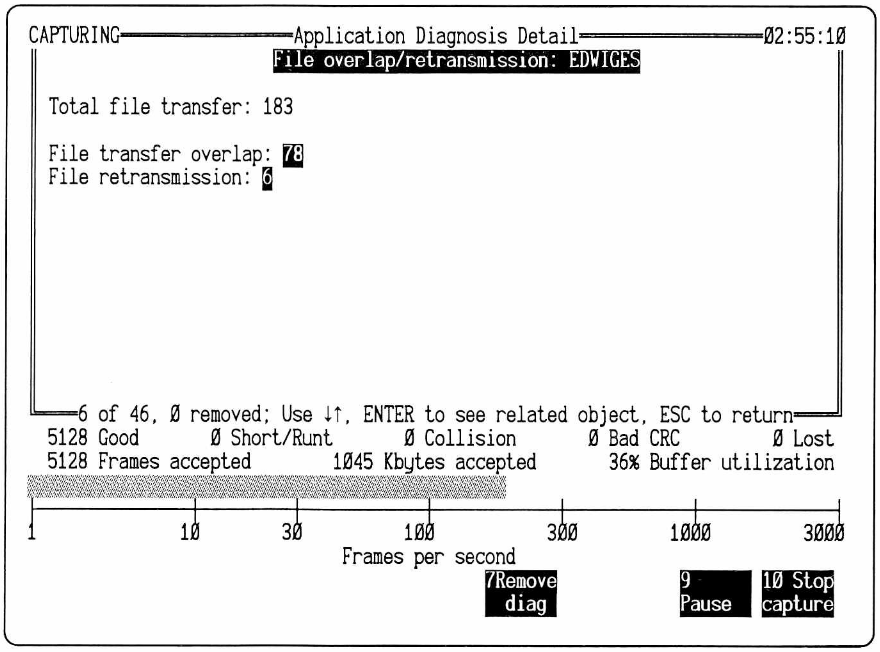
File Overlap / Retransmission

The analyzer generates the **File overlap/retransmission** diagnosis when the percentage of file transfers that are retransmissions has exceeded the **Slow file%** threshold in the **Expert Settings** menu. For more information on this threshold, see page 3–20.

This diagnosis indicates excessive retransmissions of the same file request, or overlap between two file requests. The detail display provides the following information.

- The address or symbolic name of the station sending repeated or overlapping file requests
- The total number of file transfers in which this station was involved
- The number of file transfers which were overlapping file requests
- The number of file transfers which were retransmissions

Figure 4–9 shows the detail display for the **File overlap/retransmission** diagnosis.



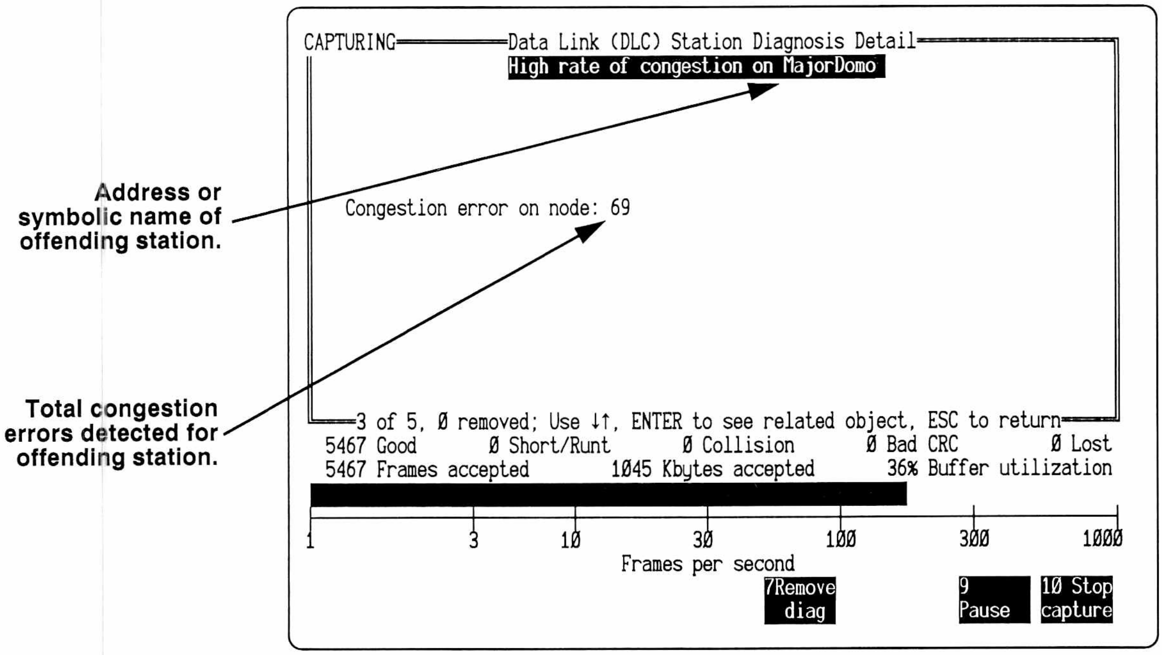
```
CAPTURING══════════Application Diagnosis Detail══════════Ø2:55:1Ø
                   File overlap/retransmission: EDWIGES

 Total file transfer: 183

 File transfer overlap: 78
 File retransmission: 6

═══6 of 46, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═══
 5128 Good        Ø Short/Runt      Ø Collision      Ø Bad CRC       Ø Lost
 5128 Frames accepted       1Ø45 Kbytes accepted     36% Buffer utilization
```

Figure 4–9. Detail display for the diagnosis, "File overlap/retransmission."

High Rate of Congestion

The analyzer generates the **High rate of congestion** diagnosis when it detects a particular station exhibiting more receiver congestion errors per minute than specified by the **RX Congestion** threshold. Receiver congestion errors occur when a station detects a frame on the ring with its own destination address but is unable to copy it because of a lack of buffer space. For more information on the **RX Congestion** threshold, see page 3–26.

Figure 4–10 shows a typical detail display for the **High rate of congestion** diagnosis. In this example, there have been 69 total receiver congestion errors detected for the station MajorDomo. The information provided by this detail display is described at the left of Figure 4–10.



```
CAPTURING═══════Data Link (DLC) Station Diagnosis Detail════════════════
                High rate of congestion on MajorDomo

    Congestion error on node: 69

════3 of 5, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═══
  5467 Good        Ø Short/Runt       Ø Collision       Ø Bad CRC       Ø Lost
  5467 Frames accepted        1Ø45 Kbytes accepted      36% Buffer utilization

1             3        1Ø          3Ø          1ØØ          3ØØ          1ØØØ
                               Frames per second
                                         7Remove            9      1Ø Stop
                                          diag            Pause    capture
```

Address or symbolic name of offending station.

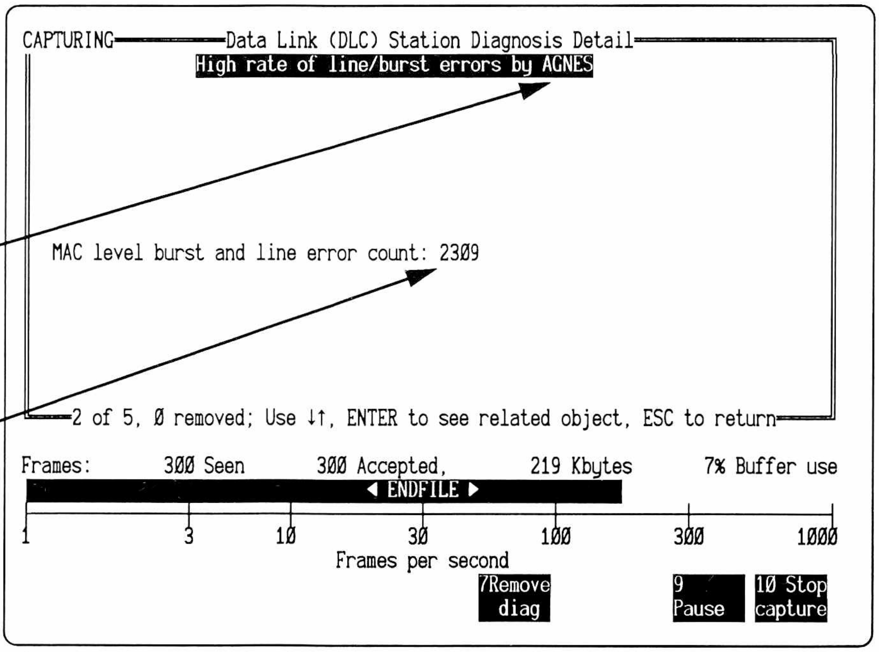
Total congestion errors detected for offending station.

Figure 4–10. Detail display for the diagnosis, "High rate of congestion."

High Rate of Line or Burst Errors

The analyzer generates the **High rate of line/burst errors** diagnosis when the total MAC level line errors plus burst errors for a particular station exceeds the **Ring errors** threshold. For more information on the **Ring errors** threshold, see page 3–27.

Figure 4–11 shows a typical detail display for the **High rate of line/burst errors** diagnosis. In this example, the station AGNES has had a total of 2309 line errors plus burst errors during this capture session. The information provided by this detail display is described at the left of Figure 4–11.



```
CAPTURING──────Data Link (DLC) Station Diagnosis Detail──────
              High rate of line/burst errors by AGNES

  MAC level burst and line error count: 23Ø9

──2 of 5, Ø removed; Use ↓↑, ENTER to see related object, ESC to return──
Frames:      3ØØ Seen      3ØØ Accepted,      219 Kbytes      7% Buffer use
                          ◀ ENDFILE ▶
1            3        1Ø        3Ø        1ØØ        3ØØ        1ØØØ
                        Frames per second
                                7Remove           9       1Ø Stop
                                 diag           Pause     capture
```

Address or symbolic name of offending station.

Total line/burst errors detected for offending station.

Figure 4–11. Detail display for the diagnosis, "High rate of line/burst errors."

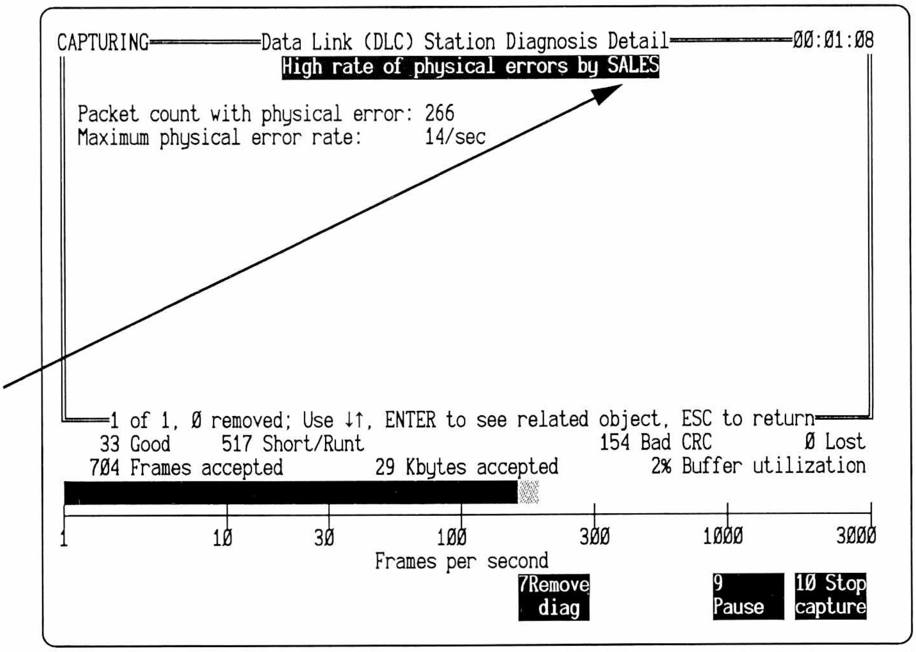
High Rate of Physical Errors

The analyzer generates the diagnosis **High rate of physical errors** when the number of physical errors per second detected for a given station exceeds the **Physical err** threshold in the Expert settings menu. For more information on how the analyzer tracks physical errors, refer to page 3–25.

The detail display for the **High rate of physical errors** diagnosis includes the following information:

Name	The address or symbolic name of the offending station.
Packet count	The total number of packets exhibiting physical errors sent by the offending station. You can press Enter to see the Network Object Detail display. That display shows both the number of physical error packets sent and received by the offending station.
Physical error rate	The maximum rate of physical error packets per second sent by the offending station.

Figure 4–12 shows a typical detail display for the **High rate of physical errors** diagnosis. In this example, the station SALES has transmitted a total of 266 packets exhibiting physical errors. The maximum rate at which these physical error packets were sent was 14/second, exceeding the default **Physical err** threshold of 4/second per station.



```
CAPTURING══════Data Link (DLC) Station Diagnosis Detail══════ØØ:Ø1:Ø8
                  High rate of physical errors by SALES

 Packet count with physical error: 266
 Maximum physical error rate:      14/sec

═1 of 1, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═
  33 Good     517 Short/Runt                   154 Bad CRC        Ø Lost
 7Ø4 Frames accepted        29 Kbytes accepted         2% Buffer utilization

1          1Ø      3Ø        1ØØ         3ØØ        1ØØØ        3ØØØ
                          Frames per second
                                 7Remove          9      1Ø Stop
                                  diag          Pause    capture
```

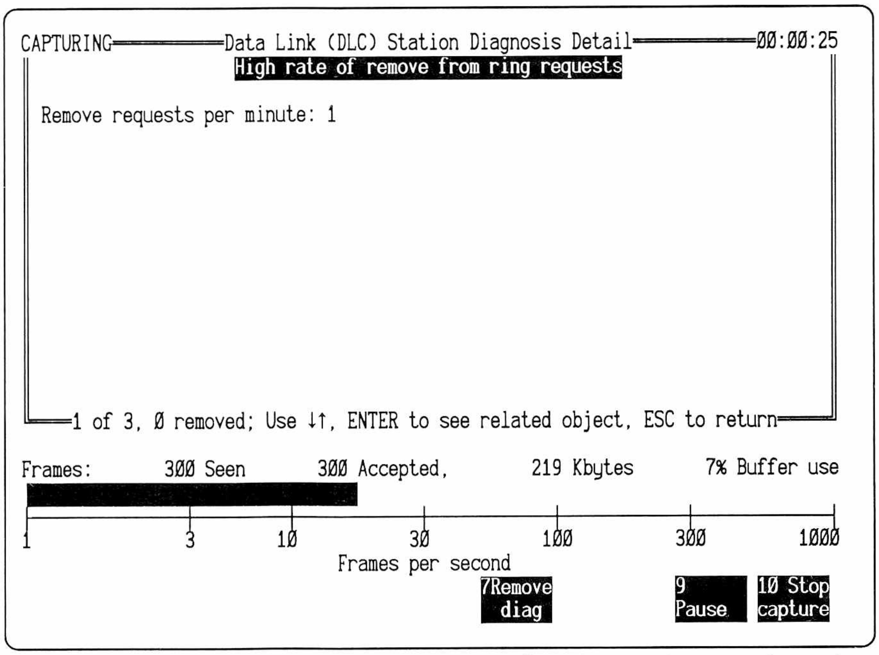
Address or symbolic name of offending station.

Figure 4–12. Detail display for the diagnosis, "High rate of physical errors."

High Rate of Remove from Ring Requests

The analyzer generates the diagnosis **High rate of remove from ring requests** when the rate of Remove from Ring requests detected by the analyzer exceeds the **Station Removed** threshold in the Expert Settings menu. Remove from Ring requests are sent by the Configuration Report Server, a virtual ring entity responsible for overall ring health. For more information on the **Station Removed** threshold, see page 3–27.

Figure 4–13 shows a typical detail display for the **High rate of remove from ring requests** diagnosis. The display shows the number of remove from ring requests per minute detected by the analyzer. Pressing Enter from this display shows the addresses of the stations to which remove from ring requests have been sent.



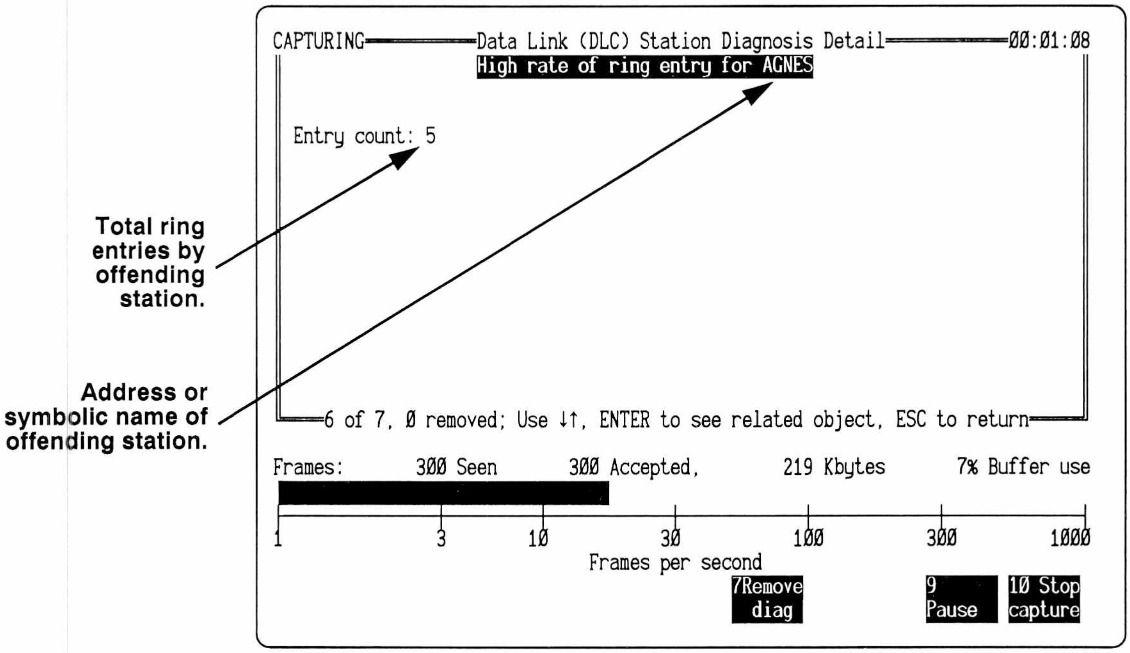
```
CAPTURING══════Data Link (DLC) Station Diagnosis Detail══════ØØ:ØØ:25
                High rate of remove from ring requests

 Remove requests per minute: 1









══1 of 3, Ø removed; Use ↓↑, ENTER to see related object, ESC to return══

Frames:      3ØØ Seen      3ØØ Accepted,       219 Kbytes      7% Buffer use

1              3        1Ø         3Ø          1ØØ          3ØØ         1ØØØ
                              Frames per second
                                         7Remove            9       1Ø Stop
                                          diag              Pause   capture
```

Figure 4–13. Detail display for the diagnosis, "High rate of remove from ring requests."

High Rate of Ring Entries

The analyzer generates the **High rate of ring entry** diagnosis when the number of ring entries per minute for a given station exceeds the **Ring entries** threshold. For more information on the **Ring entries** threshold, see page 3–26.

Figure 4–14 shows a typical detail display for the **High rate of ring entry** diagnosis. In this example, the station AGNES has entered the ring five times. The information provided by this display is described at the left of Figure 4–14.



```
CAPTURING═══════Data Link (DLC) Station Diagnosis Detail═══════00:01:08
                High rate of ring entry for AGNES

  Entry count: 5

═══6 of 7, 0 removed; Use ↓↑, ENTER to see related object, ESC to return═══
Frames:       300 Seen      300 Accepted,      219 Kbytes       7% Buffer use

1          3      10        30         100        300        1000
                       Frames per second
```

Total ring entries by offending station.

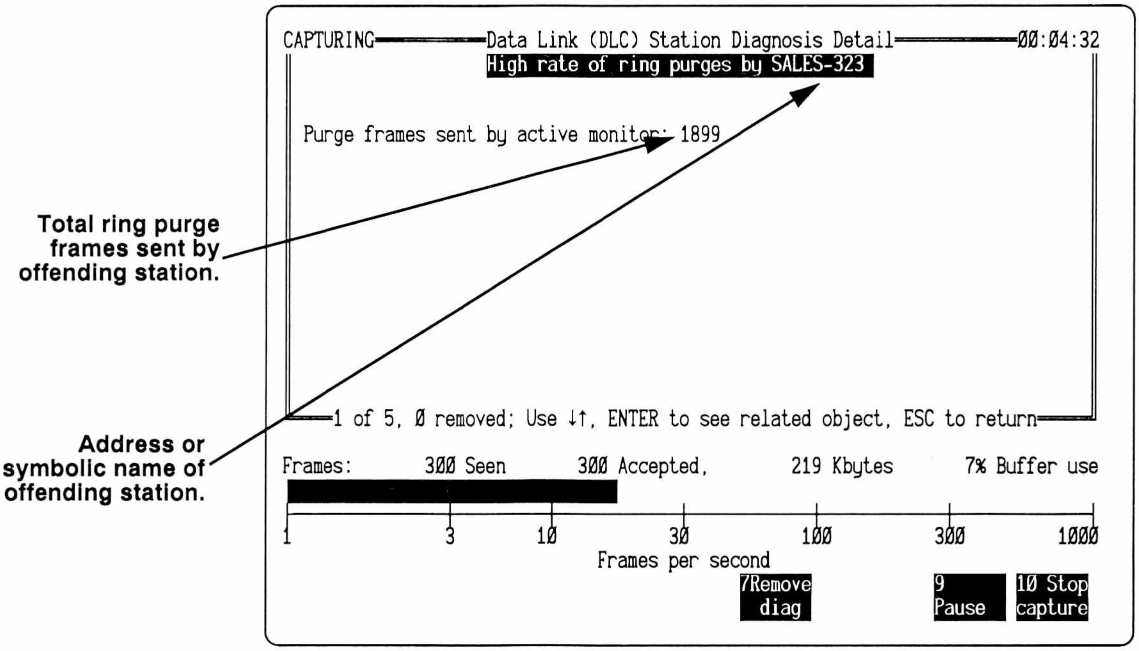
Address or symbolic name of offending station.

Figure 4–14. Detail display for the diagnosis, "High rate of ring entry."

High Rate of Ring Purges

The analyzer generates the **High rate of ring purges** diagnosis when the number of purge frames per minute sent by a given station exceeds the threshold specified by **Rng purge dg** in the Expert settings menu. Ring purge frames are sent by the active monitor when it detects that a token has been lost. For more information on the **Rng purge dg** threshold, see page 3–27.

Figure 4–15 shows a typical detail display for the **High rate of ring purges** diagnosis. In this example, the station SALES-323 has sent a total of 1899 ring purge frames during this capture session. The information in the detail display for this diagnosis is described at the left of Figure 4–15.



```
CAPTURING═══════Data Link (DLC) Station Diagnosis Detail═══════ØØ:Ø4:32
                High rate of ring purges by SALES-323

  Purge frames sent by active monitor: 1899

═1 of 5, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═
Frames:      3ØØ Seen      3ØØ Accepted,      219 Kbytes      7% Buffer use
1            3        1Ø        3Ø        1ØØ        3ØØ        1ØØØ
                         Frames per second
                             7Remove              9        1Ø Stop
                              diag              Pause      capture
```

Total ring purge frames sent by offending station.

Address or symbolic name of offending station.

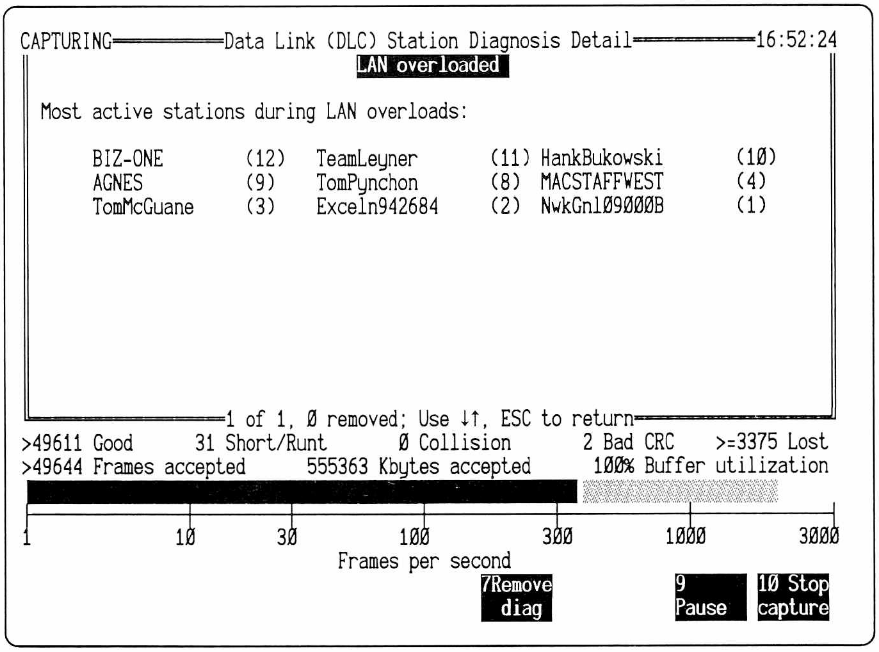
Figure 4–15. Detail display for the diagnosis, "High rate of ring purges."

LAN Overloaded

The analyzer generates the **LAN overloaded** diagnosis when the percentage of each minute the network is in burst mode exceeds the **LAN overload %** threshold. Whether the network is considered to be in burst mode depends on the setting of the **LAN overload** threshold. For a detailed discussion of these two thresholds and how they interact, see page 3–24.

Because the **LAN overloaded** diagnosis is directly related to the quantity of **Network overload** symptoms, the detail display shows the name or symbolic address of each network station whose traffic is associated with a **Network overload** symptom. Included in the display is the exact number of **Network overload** symptoms with which each particular station is associated. The stations are organized in descending order. Figure 4–25 shows the detail display for the **LAN overloaded** diagnosis.

Each listed station is associated with one or more Network overload symptoms. The number in parentheses shows exactly how many. Notice that the stations are organized in descending order.



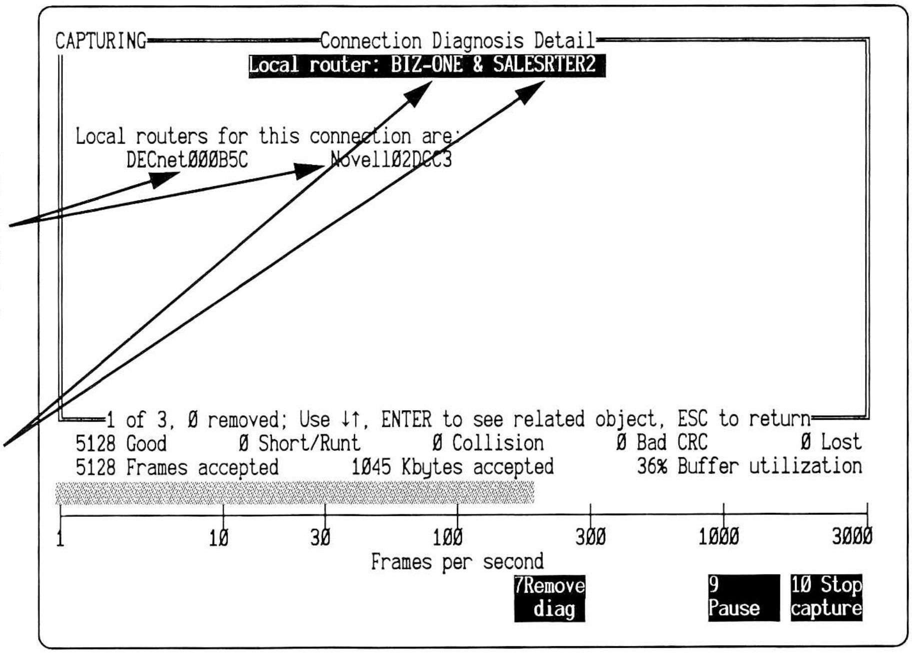
```
CAPTURING══════════Data Link (DLC) Station Diagnosis Detail══════════16:52:24
                              LAN overloaded

 Most active stations during LAN overloads:

      BIZ-ONE        (12)   TeamLeyner        (11) HankBukowski      (1Ø)
      AGNES          (9)    TomPynchon        (8)  MACSTAFFWEST      (4)
      TomMcGuane     (3)    Exceln942684      (2)  NwkGnl Ø9ØØØB     (1)

══════════════════1 of 1, Ø removed; Use ↓↑, ESC to return═════════════════
>49611 Good      31 Short/Runt       Ø Collision       2 Bad CRC    >=3375 Lost
>49644 Frames accepted      555363 Kbytes accepted      1ØØ% Buffer utilization

1              1Ø        3Ø         1ØØ         3ØØ         1ØØØ         3ØØØ
                                Frames per second
                                      7Remove                9       1Ø Stop
                                       diag                  Pause   capture
```

Figure 4–16. Detail display for the diagnosis, "LAN overloaded."

Local Router

The analyzer generates the diagnosis **Local router** when two DLC stations on the same network segment are communicating via one or more routers, rather than directly from one DLC station to the other.

The detail display for this diagnosis is shown in Figure 4–17. The information in the detail display is described at the left of Figure 4–17.



```
CAPTURING══════════════Connection Diagnosis Detail════════════════════
                     Local router: BIZ-ONE & SALESRTER2

  Local routers for this connection are:
      DECnet000B5C            Novell02DCC3

══1 of 3, 0 removed; Use ↓↑, ENTER to see related object, ESC to return══
  5128 Good         0 Short/Runt      0 Collision       0 Bad CRC        0 Lost
  5128 Frames accepted      1045 Kbytes accepted        36% Buffer utilization
```

Addresses or symbolic names of local routers through which DLC stations communicate unnecessarily.

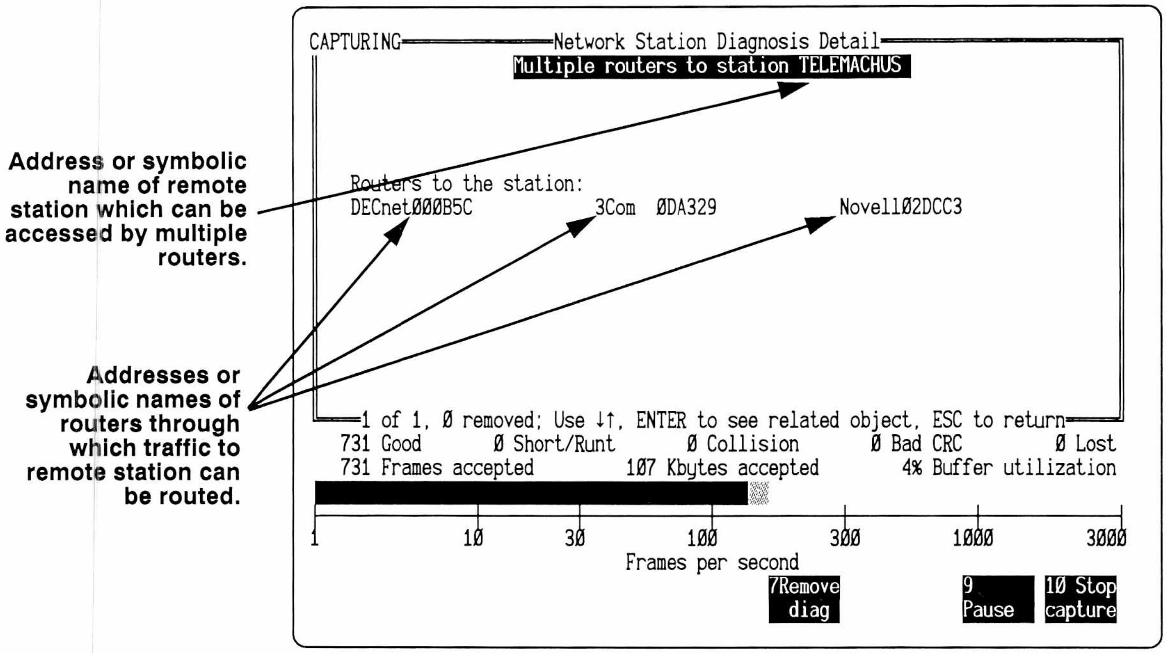
Addresses or symbolic names of DLC stations communicating through local routers rather than directly.

Figure 4–17. Detail display for the diagnosis, "Local Router."

Multiple Routers to Station

The analyzer generates the diagnosis **Multiple routers to station** *address* when there are more routers on the local network that can route to a remote station than specified by the **Multiple routers** threshold in the **Expert Settings** menu. For more information on the **Multiple routers** threshold, see page 3–22.

The detail display for the diagnosis **Multiple routers to station** is shown in Figure 4–18. The information in the detail display is described at the left of Figure 4–18.



```
CAPTURING══════════════Network Station Diagnosis Detail══════════════
                    Multiple routers to station TELEMACHUS

Routers to the station:
DECnet000B5C            3Com  0DA329            Novell02DCC3

════1 of 1, 0 removed; Use ↓↑, ENTER to see related object, ESC to return════
  731 Good        0 Short/Runt      0 Collision       0 Bad CRC        0 Lost
  731 Frames accepted        107 Kbytes accepted        4% Buffer utilization

1           10        30        100        300       1000        3000
                          Frames per second
                              7Remove              9       10 Stop
                               diag                Pause   capture
```

Address or symbolic name of remote station which can be accessed by multiple routers.

Addresses or symbolic names of routers through which traffic to remote station can be routed.

Figure 4–18. Detail display for the diagnosis, "Multiple routers to station."

Non-Responsive Station

The analyzer generates the diagnosis **Non-responsive station** (and considers a connection broken) when the number of consecutive identical retransmissions without response on a given connection exceeds the **No Responses** threshold in the **Expert Settings** menu.

The analyzer considers a broken connection to start when the number of retransmissions exceeds the **No responses** threshold and to end when the sender sends a new packet. Figure 4–19 illustrates how the analyzer calculates the duration of a broken connection.

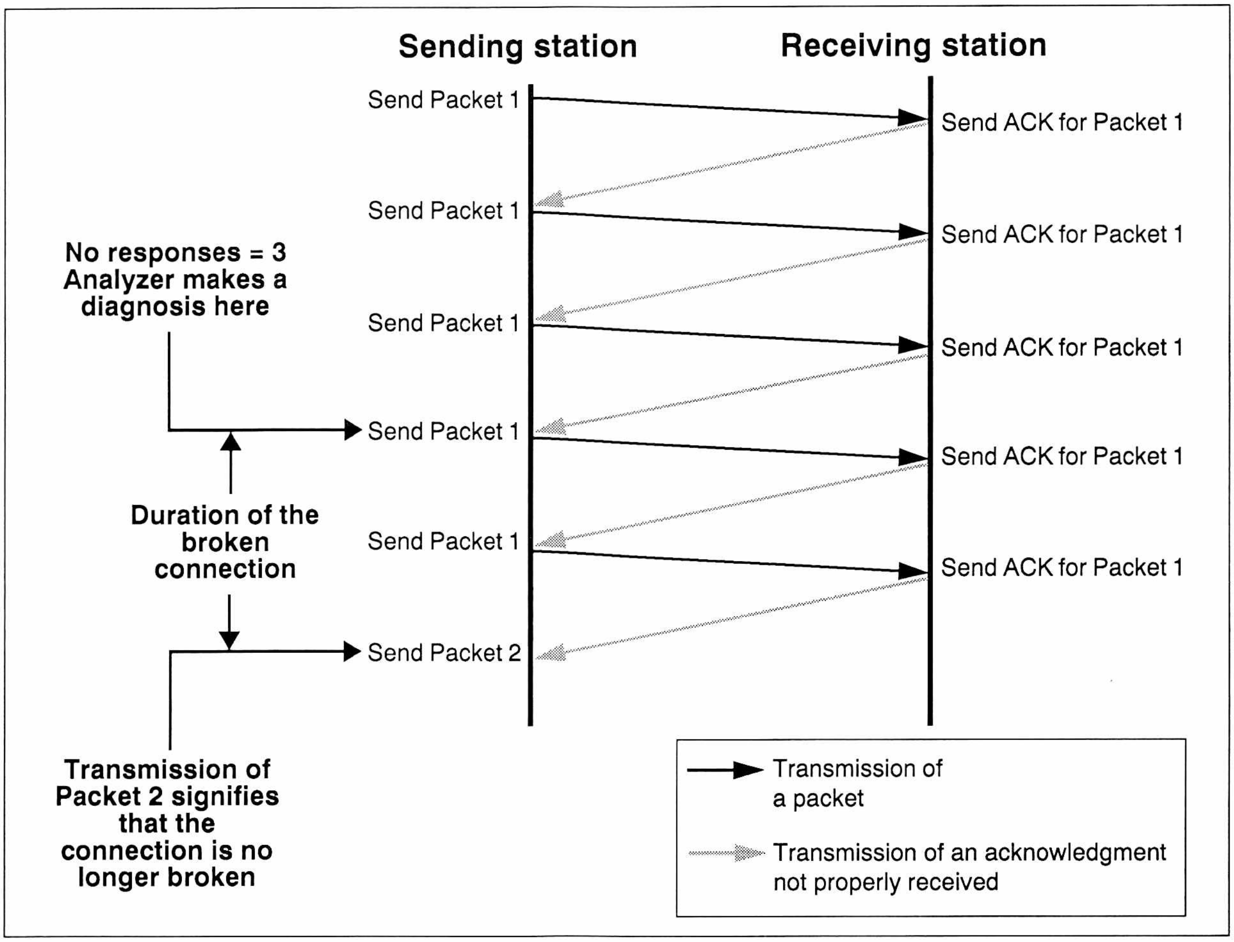
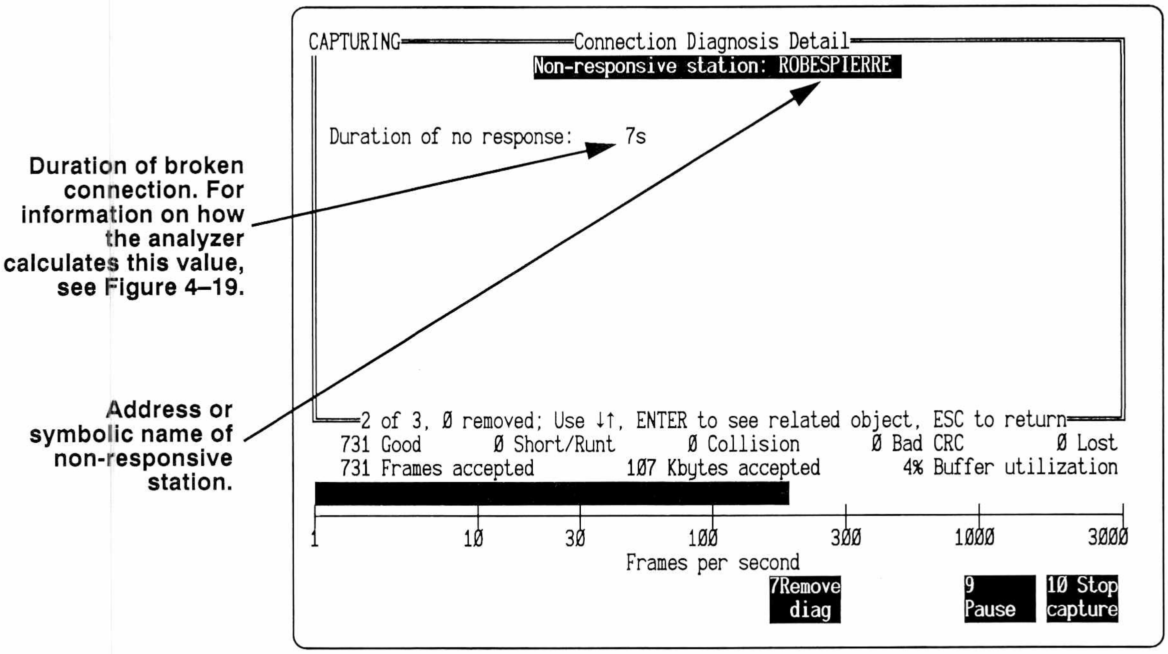


Figure 4–19. How the analyzer calculates a broken connection.

Figure 4–20 shows the detail display for the diagnosis **Non-responsive station.** For more information on the **No responses** threshold, see page 3–21.



```
CAPTURING═══════════Connection Diagnosis Detail═══════════════
                   Non-responsive station: ROBESPIERRE

  Duration of no response:    7s

═══2 of 3, Ø removed; Use ↓↑, ENTER to see related object, ESC to return═══
  731 Good        Ø Short/Runt      Ø Collision      Ø Bad CRC        Ø Lost
  731 Frames accepted        1Ø7 Kbytes accepted        4% Buffer utilization
```

1
1Ø
3Ø
1ØØ
3ØØ
1ØØØ
3ØØØ
Frames per second
7Remove diag
9 Pause
1Ø Stop capture
Duration of broken connection. For information on how the analyzer calculates this value, see Figure 4–19.
Address or symbolic name of non-responsive station.

Figure 4–20. Detail display for the diagnosis, "Non-responsive station."

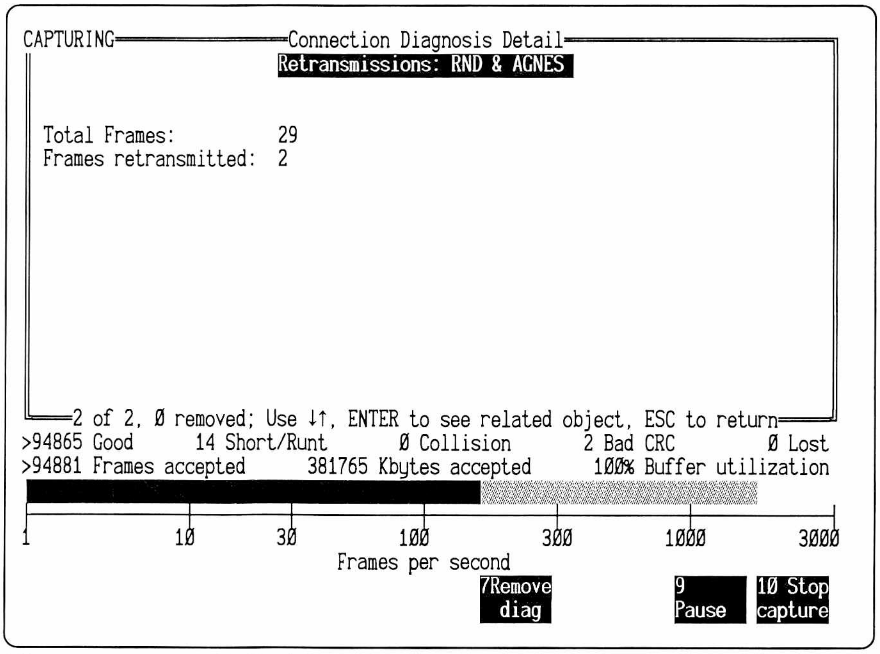
Retransmissions

The analyzer generates the **Retransmissions** diagnosis when the number of retransmissions (expressed as a percentage of total frames on the connection) exceeds the **Retrans %** threshold. For more information on the **Retrans %** threshold, see page 3–21.

The detail display for the **Retransmissions** diagnosis provides the following information:

- The addresses or symbolic names of the endpoint of the connection exhibiting the **Retransmission** diagnosis
- The total number of frames sent on this connection
- The number of frames retransmitted on this connection

Figure 4–21 shows a typical detail display for the **Retransmissions** diagnosis. In this example, 29 frames have passed between the server RND and the workstation AGNES. Of these 29 frames, two were retransmissions.



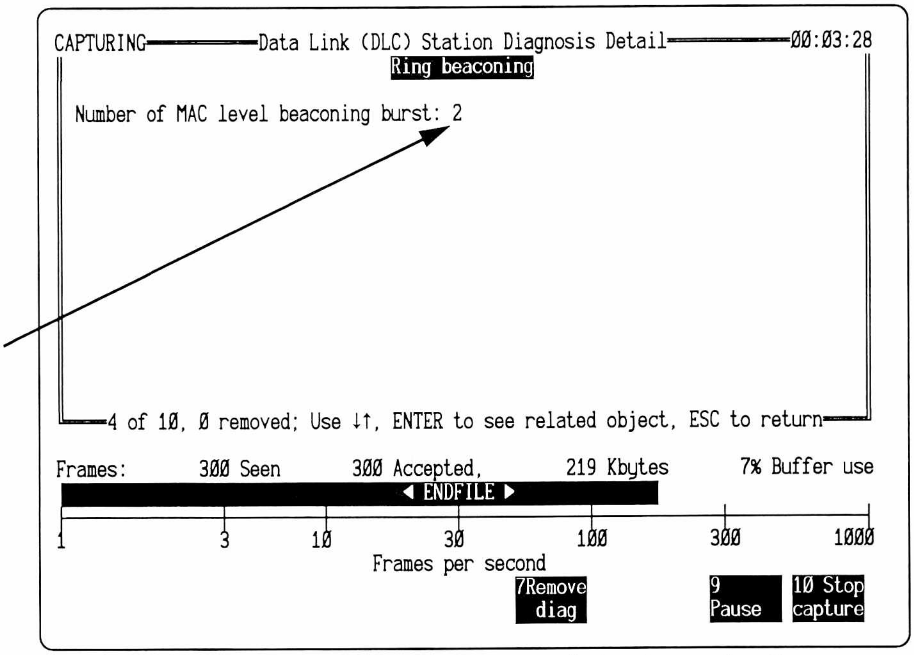
```
CAPTURING==============Connection Diagnosis Detail=====================
                       Retransmissions: RND & AGNES

  Total Frames:           29
  Frames retransmitted:   2

=====2 of 2, 0 removed; Use ↓↑, ENTER to see related object, ESC to return====
>94865 Good       14 Short/Runt       0 Collision      2 Bad CRC        0 Lost
>94881 Frames accepted      381765 Kbytes accepted      100% Buffer utilization
```

Figure 4–21. Detail display for the diagnosis, "Retransmissions."

Ring Beaconing

The analyzer generates the **Ring beaconing** diagnosis when it detects a single MAC beacon frame. Beacon frames indicate that there is a problem in the token ring that makes the ring inoperable. A ring can be beaconing due to a physical break in the ring or a timeout during active monitor contention.

The information at the left of Figure 4–22 describes the contents of a typical detail display for the **Ring beaconing** diagnosis.



```
CAPTURING————Data Link (DLC) Station Diagnosis Detail————ØØ:Ø3:28
                          Ring beaconing

 Number of MAC level beaconing burst: 2

——4 of 1Ø, Ø removed; Use ↓↑, ENTER to see related object, ESC to return——

Frames:      3ØØ Seen      3ØØ Accepted,      219 Kbytes      7% Buffer use
                             ◀ ENDFILE ▶
1          3        1Ø         3Ø         1ØØ        3ØØ        1ØØØ
                        Frames per second
                               7Remove               9       1Ø Stop
                                diag                 Pause   capture
```

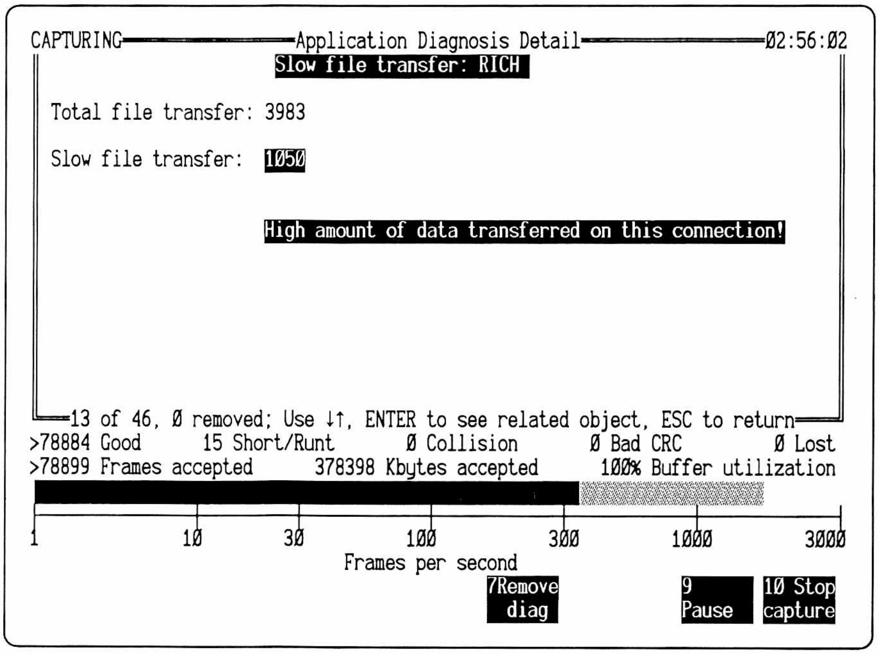
Number of MAC level beacon frames detected by the analyzer.

Figure 4–22. Detail display for the diagnosis, "Ring beaconing."

Slow File Transfer

The analyzer generates the **Slow file transfer** diagnosis when the ratio of slow versus normal file transfers is greater than the **Slow file** % threshold in the Expert settings menu. For more information on this threshold and how the analyzer determines whether a file transfer is "slow," see the "Denied Request Percentage" and "Slow File Percentage" sections, starting on page 3–19.

The detail display for the **Slow file transfer** diagnosis shows the address or symbolic name of the station that requests the file transfer, as well as the number of slow file transfers versus total file transfers. Figure 4–23 shows a typical detail screen for the **Slow file transfer** diagnosis.



```
CAPTURING─────────────Application Diagnosis Detail──────────────Ø2:56:Ø2
                      Slow file transfer: RICH

  Total file transfer: 3983

  Slow file transfer:  1Ø5Ø

                      High amount of data transferred on this connection!

──13 of 46, Ø removed; Use ↓↑, ENTER to see related object, ESC to return──
>78884 Good        15 Short/Runt       Ø Collision      Ø Bad CRC      Ø Lost
>78899 Frames accepted      378398 Kbytes accepted      1ØØ% Buffer utilization

1          1Ø      3Ø       1ØØ       3ØØ       1ØØØ       3ØØØ
                       Frames per second
                                7Remove             9       1Ø Stop
                                 diag             Pause     capture
```

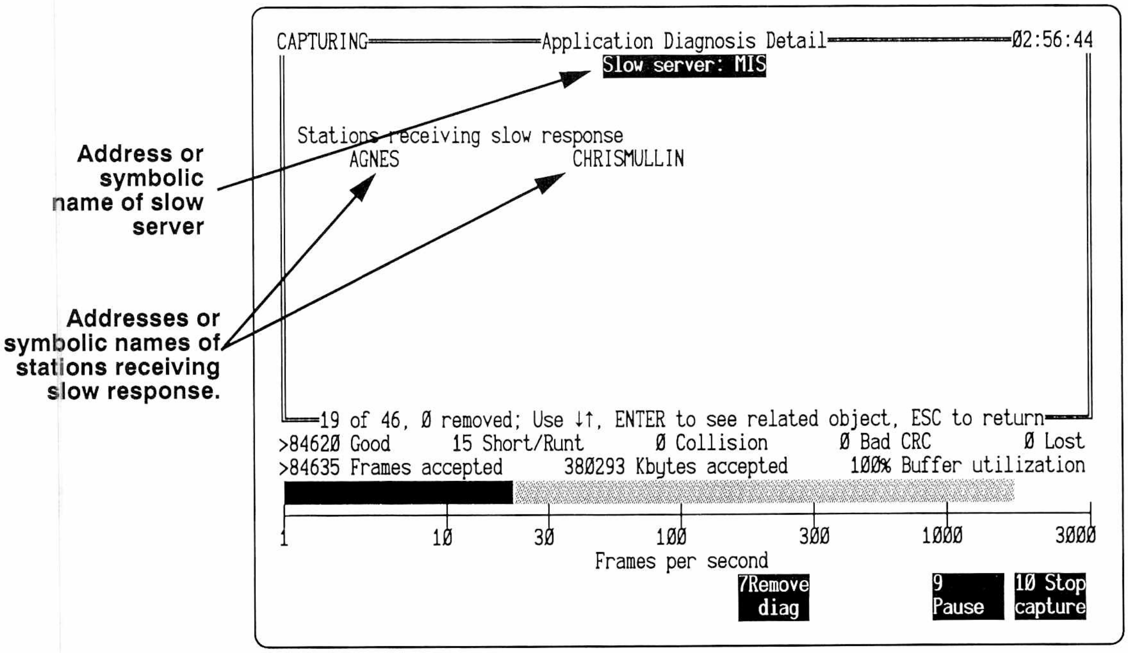
Figure 4–23. Detail display for the diagnosis, "Slow file transfer."

In Figure 4–23, notice that the analyzer has printed the message, "`High amount of data transferred on this connection!`" When the Expert analyzer notices a network event it considers particularly troublesome, it will sometimes print a warning message directly on the screen. In this case, the workstation, "RICH," is involved in a dangerously high-traffic connection. To view statistics on this connection, press Enter to see the Application Detail screen containing the address of the server responding to Rich's requests and any symptoms that may be associated with this connection.

Slow Server

The analyzer generates the **Slow server** diagnosis when the ratio of slow responses to total responses for a particular station exceeds the **Slow resp %** threshold in the Expert settings menu. For more information on this threshold and how the analyzer determines whether a response is "slow," see the "Minimum Application Requests" and "Response Time" sections, starting on page 3–17.

The detail display for the **Slow server** diagnosis shows the name or symbolic address of the slow server. The display also shows the name or symbolic address of each station that has received a slow response from the named server. The analyzer adds a station name to the list as soon as it detects that the station has received a slow response from this server. Figure 4–24 shows the detail display for the **Slow server** diagnosis.



```
CAPTURING══════════════Application Diagnosis Detail═══════════════Ø2:56:44
                                   Slow server: MIS

   Stations receiving slow response
        AGNES                        CHRISMULLIN

══19 of 46, Ø removed; Use ↓↑, ENTER to see related object, ESC to return══
>8462Ø Good        15 Short/Runt        Ø Collision       Ø Bad CRC        Ø Lost
>84635 Frames accepted      38Ø293 Kbytes accepted      1ØØ% Buffer utilization

1            1Ø        3Ø          1ØØ          3ØØ         1ØØØ        3ØØØ
                              Frames per second
```

Address or symbolic name of slow server

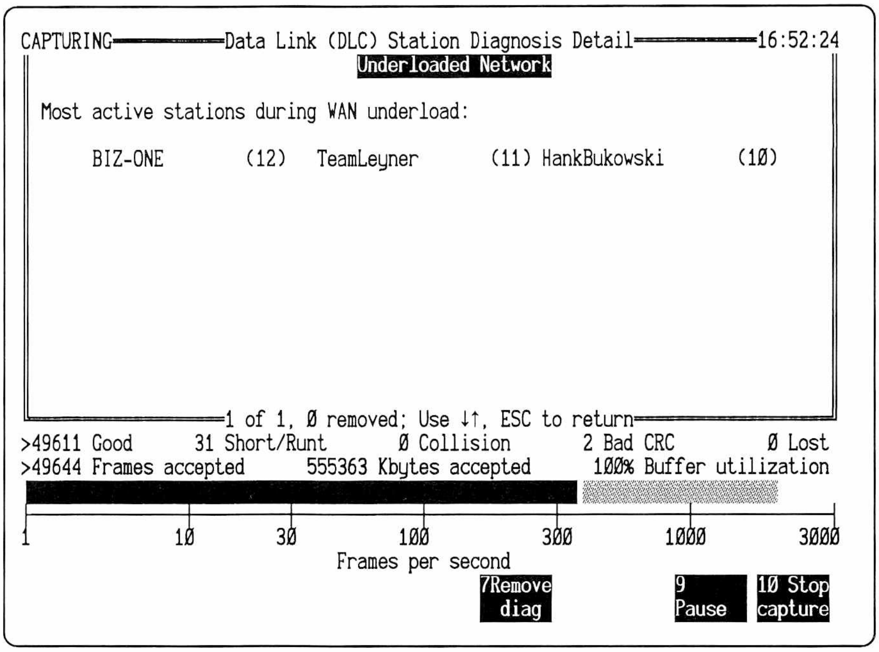
Addresses or symbolic names of stations receiving slow response.

Figure 4–24. Detail display for the diagnosis, "Slow server."

Underloaded Network

The analyzer generates the **Underloaded network** diagnosis when the duration of an underload condition exceeds the **Underload Timer** threshold. Whether the network is considered to be in an underload condition depends on the setting of the **WAN underload** threshold. If the network load (for both DTE and DCE) is less than that specified by **WAN underload**, then the analyzer considers the network to be in an underload condition. For a detailed discussion of these two thresholds and how they interact, see page 3–28.

The detail display shows the name or symbolic address of the most active stations during the WAN underload.



```
CAPTURING════════Data Link (DLC) Station Diagnosis Detail════════16:52:24
                                   Underloaded Network

 Most active stations during WAN underload:

      BIZ-ONE        (12)  TeamLeyner      (11) HankBukowski        (10)

═══════════════════1 of 1, 0 removed; Use ↓↑, ESC to return══════════════════
>49611 Good       31 Short/Runt       0 Collision       2 Bad CRC        0 Lost
>49644 Frames accepted      555363 Kbytes accepted      100% Buffer utilization
```

Figure 4–25. Detail display for the diagnosis, "Underloaded network."

Symptom and Network Object-Related Displays

This section describes the various displays accessible from the **Objects/Symptoms** column of the Expert Overview. The Expert displays accessible from the **Diagnoses** column of the Expert Overview are described starting on page 4–10. Note that the same displays are available in the Expert window regardless of whether the analyzer is capturing or displaying frames.

You may want to refer to Figure 4–1 on page 4–4 for a schematic of the various Expert windows and how they relate to one another.

About Symptom and Network Object-Related Displays

Symptom and Network Object displays are similar to the various diagnosis-related displays, except that:

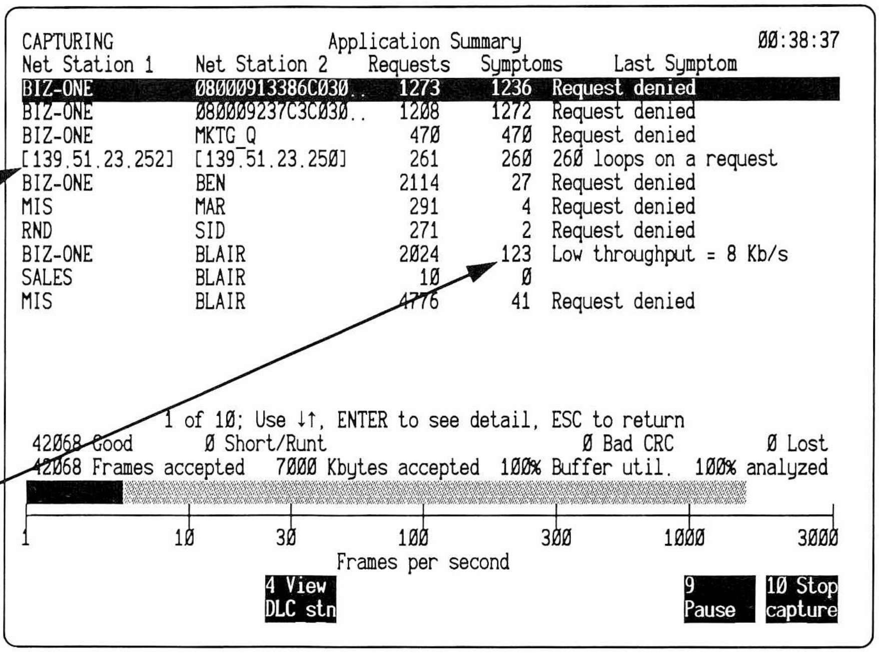
- The counts pertain to symptoms detected, not diagnoses.
- Even if no symptoms are detected at a particular layer, you can still select that layer and press Enter to display a list of connections, network addresses, or DLC addresses.
- The **Objects/Symptoms** column also displays pairs of communicating subnets. You can highlight the subnet field and press Enter to see a list of communicating subnet pairs. (The purpose of this field is to provide more information about the subnets; symptoms are not associated with subnets.)
- The **Objects/Symptoms** column also displays Global Symptoms. Global symptoms include LAN and WAN Overloads.

You can navigate through the symptom and network object-related displays just as you would the diagnosis-related displays. Highlighting a field and pressing Enter causes a Summary window to appear. However, the Symptom and Network Object Summary displays are different from the Diagnosis Summary displays, inasmuch as they display a list of *all* network objects detected by the Expert analyzer instead of just those exhibiting symptoms.

Symptom and Network Object Summary Windows

Symptom and Network Object Summary windows provide a list of all network objects detected by the Expert analyzer at the highlighted Expert layer. The Summary windows act as a gateway to the more detailed windows, summarizing general data about the various applications, connections, network stations, and DLC stations detected by the analyzer.

For example, Figure 4–26 shows the Summary window at the Expert Application layer. It lists all the Application layer connections detected by the analyzer during this capture session, the addresses of the connecting stations, the number of frames that have passed between the two stations, and the number of symptoms associated with those frames. From here, the display shows that the connection between the workstation, BLAIR, and the server BIZ-ONE currently has 123 associated symptoms, including the last symptom detected, **Low throughput**. You can explore this connection further by highlighting it and pressing Enter to see the related Detail window.



```
CAPTURING                     Application Summary                         ØØ:38:37
Net Station 1     Net Station 2   Requests  Symptoms      Last Symptom
BIZ-ONE           Ø8ØØØ913386CØ3Ø..  1273      1236  Request denied
BIZ-ONE           Ø8ØØØ9237C3CØ3Ø..  12Ø8      1272  Request denied
BIZ-ONE           MKTG_Q              47Ø       47Ø  Request denied
[139.51.23.252]   [139.51.23.25Ø]     261       26Ø  26Ø loops on a request
BIZ-ONE           BEN                2114        27  Request denied
MIS               MAR                 291         4  Request denied
RND               SID                 271         2  Request denied
BIZ-ONE           BLAIR              2Ø24       123  Low throughput = 8 Kb/s
SALES             BLAIR                1Ø         Ø
MIS               BLAIR              4776        41  Request denied




                 1 of 1Ø; Use ↓↑, ENTER to see detail, ESC to return
 42Ø68 Good          Ø Short/Runt                           Ø Bad CRC         Ø Lost
42Ø68 Frames accepted   7ØØØ Kbytes accepted  1ØØ% Buffer util.  1ØØ% analyzed
```

Addresses or symbolic names of connecting stations

The BIZ-ONE–BLAIR connection currently has 123 associated symptoms.

Figure 4–26. Symptom and Network Object Summary window at the Expert Application layer.

Displaying the Summary Window

The following procedure describes how to display the Summary window at any of the Expert layers.

To display a Summary window at any of the Expert layers:

1. From the Symptom and Network Object Overview, use the cursor keys to highlight the desired Expert layer. The available Expert layers include:
   - Application Layer
   - Connection Layer
   - Network Station Layer
   - Subnet Pairs
   - DLC Station Layer
   - Global Symptoms

   Note: Subnet Pairs and **Global Symptoms** are not true Expert layers. The purpose of these fields is to provide more information about communicating subnet pairs and global symptoms, such as traffic bursts.

2. Press Enter.

   Result: The Summary window for the selected layer appears, displaying a list of connections, network addresses, or DLC addresses. The exact format of the display depends on the Expert layer selected.

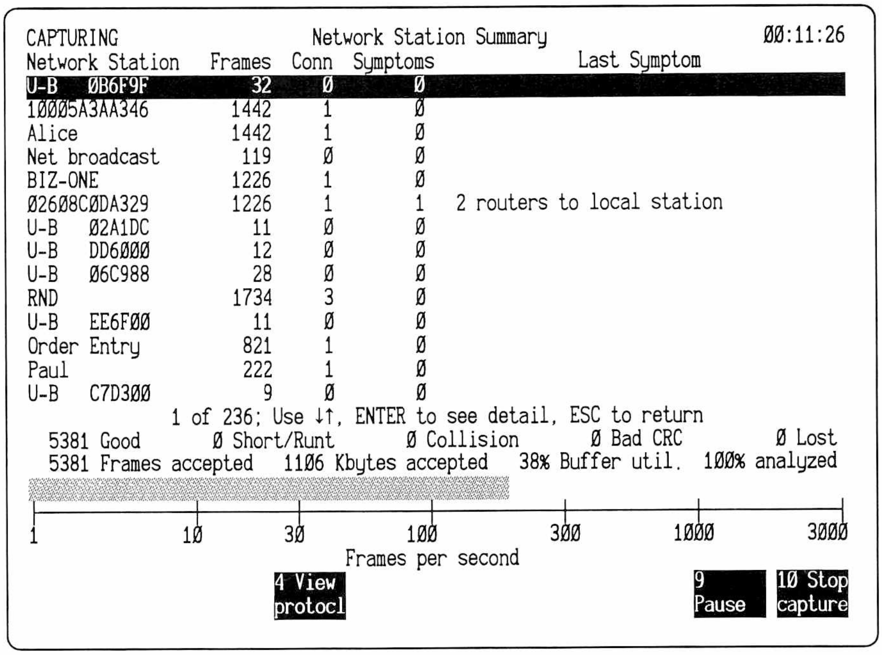
Result: The Summary window for the selected layer appears, displaying a list of connections, network addresses, or DLC addresses. The exact format of the display depends on the Expert layer selected.

Information in the Summary Windows

The information presented in the Summary windows is very similar at each of the four Expert layers. However, the Subnet Pairs and Global Symptom windows are slightly different. Those windows are described in later sections.

The Summary windows for the Network Station and DLC layers will contain less information than those at the Application and Connection layers. This is because the analyzer detects information for single stations at the Network Station and DLC layers, whereas at the Application and Connection layers it detects information about connections between two stations. This means that there is twice as much address information to present in the Summary windows for these Expert layers.

Figure 4–27 is an example of the Summary window at the Network Station layer. Notice that the information presented is very similar to that in Figure 4–26 but for only one station.



```
CAPTURING                    Network Station Summary                          ØØ:11:26
Network Station   Frames  Conn  Symptoms                    Last Symptom
U-B   ØB6F9F          32     Ø         Ø
1ØØØ5A3AA346        1442     1         Ø
Alice               1442     1         Ø
Net broadcast        119     Ø         Ø
BIZ-ONE             1226     1         Ø
Ø26Ø8CØDA329        1226     1         1   2 routers to local station
U-B   Ø2A1DC          11     Ø         Ø
U-B   DD6ØØØ          12     Ø         Ø
U-B   Ø6C988          28     Ø         Ø
RND                 1734     3         Ø
U-B   EE6FØØ          11     Ø         Ø
Order Entry          821     1         Ø
Paul                 222     1         Ø
U-B   C7D3ØØ           9     Ø         Ø
             1 of 236; Use ↓↑, ENTER to see detail, ESC to return
  5381 Good        Ø Short/Runt       Ø Collision        Ø Bad CRC          Ø Lost
  5381 Frames accepted   11Ø6 Kbytes accepted   38% Buffer util.  1ØØ% analyzed
```

Figure 4–27. Network Station Summary window.

Information Fields in the Summary Windows

The list below summarizes (in alphabetical order) the information fields found in the Summary windows. Not all the information described here is found in every screen. The exact information in the Summary window depends on the Expert layer and the object highlighted.

Bytes

Can be either "Sent bytes," or "Received bytes." Specifies the number of bytes sent or received by the corresponding station. Available only in Network Station or DLC Station Summary window.

Conn

The total number of connections made by this station.

DLC Station Address

The DLC addresses of the server, router, or other devices involved in the connection. When the DLC address is not the same as the network address, the analyzer will display the address in parentheses. This can happen when frames are routed to a station from a remote segment. In that case, the analyzer displays the DLC address and name of the router rather than that of the remote station (the net station address will be the actual address of the remote station). See Figure 4–40 on page 4–51 for a graphic representation of this phenomenon.

The analyzer will also display a + sign in front of those DLC stations which have been reached by more than one router.

Frames

In the Connection Summary window, Frames is the total number of frames transmitted on the specified connection. In the Network Station and DLC Station Summary windows, Frames is measured separately for frames sent and frames received by each station detected by the Expert analyzer.

Last Symptom

A one-line identifier of the last symptom associated with this connection or station.

Net Station Address

The network addresses of the stations involved in the connection. If the Expert analyzer has learned the names associated with the addresses, it will display them instead of the hex, IP, or DECnet addresses.

The analyzer automatically attempts to interpret the first three bytes of the address as the name of the NIC's manufacturer. When it is able to find the manufacturer's code in its table of manufacturers, the analyzer replaces the first three bytes of the station address with an ASCII abbreviation of the manufacturer's name. For example, in Figure 4–28, the characters, "NwkGnl," are substituted for the hex characters 000065.

Protocol

A one-line identifier of the protocol used on a connection or by a station. If the analyzer does not recognize the protocol in use, it will substitute the well-know port name (which is usually also a protocol name, such as Telnet or FTP).

Requests — The number of application requests made on the highlighted connection.

Symptoms — The total number of symptoms associated with this connection or station.

Keep in mind that the Expert analyzer will dynamically update the Summary window as it learns more about the network to which it is attached. For example, as soon as the analyzer knows the symbolic name associated with a station address, it will substitute that name for the hex address.

Changing the Format of the Summary Window

The information found in each Summary window is a subset of the information in the list above. However, you can vary the information fields in the Summary window at all four Expert layers:

- Application
- Connection
- Network Station
- DLC Station

The following procedure explains how to change the format of the Summary window.

To change the format of the Summary window:

1. Display the Summary window for the desired layer. See page 4–37 for complete instructions.

   Result: Depending on the layer of the Summary window, a label for the function key F4 appears at the bottom of the display. The label for the function key will change depending on the display format it will bring up next. For example, in one view it reads, "View DLC Stn," and in another, "View protocl."

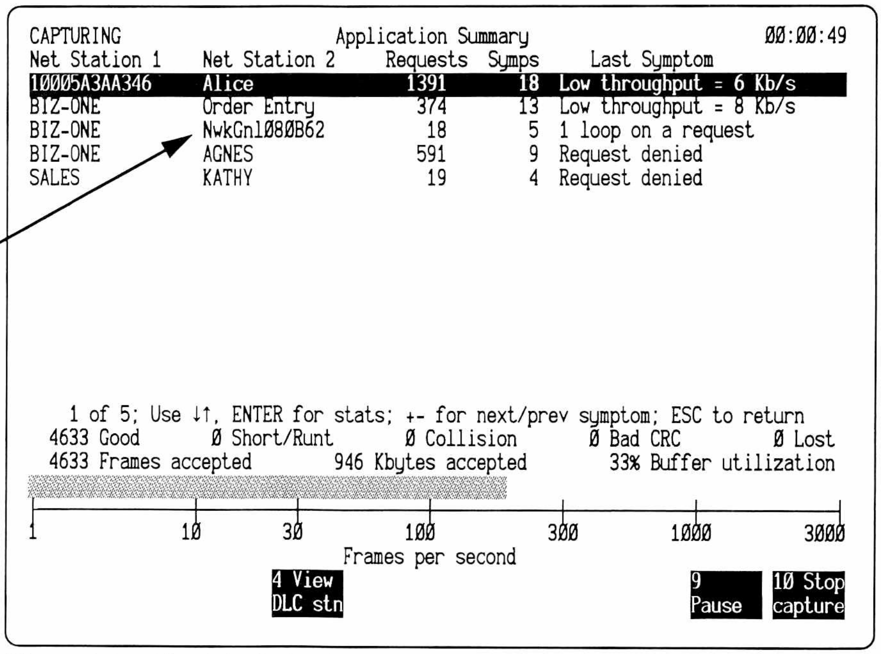
2. Press F4.

   Result: Pressing F4 allows you to cycle through the Summary display formats available at the specified layer. Each time you press F4, the information fields in the Summary window will change.

The following sections describe the various display formats available in the Summary window for each Expert layer.

Application and Connection Layer Summary Window

Figure 4–28 shows the default format for the Application Summary window.



```
CAPTURING                        Application Summary                     00:00:49
Net Station 1    Net Station 2    Requests  Symps     Last Symptom
100005A3AA346    Alice               1391     18   Low throughput = 6 Kb/s
BIZ-ONE          Order Entry          374     13   Low throughput = 8 Kb/s
BIZ-ONE          NwkGnl080B62          18      5   1 loop on a request
BIZ-ONE          AGNES                591      9   Request denied
SALES            KATHY                 19      4   Request denied

   1 of 5; Use ↓↑, ENTER for stats; +- for next/prev symptom; ESC to return
  4633 Good        0 Short/Runt        0 Collision        0 Bad CRC        0 Lost
  4633 Frames accepted        946 Kbytes accepted        33% Buffer utilization

1           10      30         100        300        1000        3000
                          Frames per second
```

The analyzer interprets the first three bytes of an address as the name of the manufacturer.

Figure 4–28. The default Application Summary window.

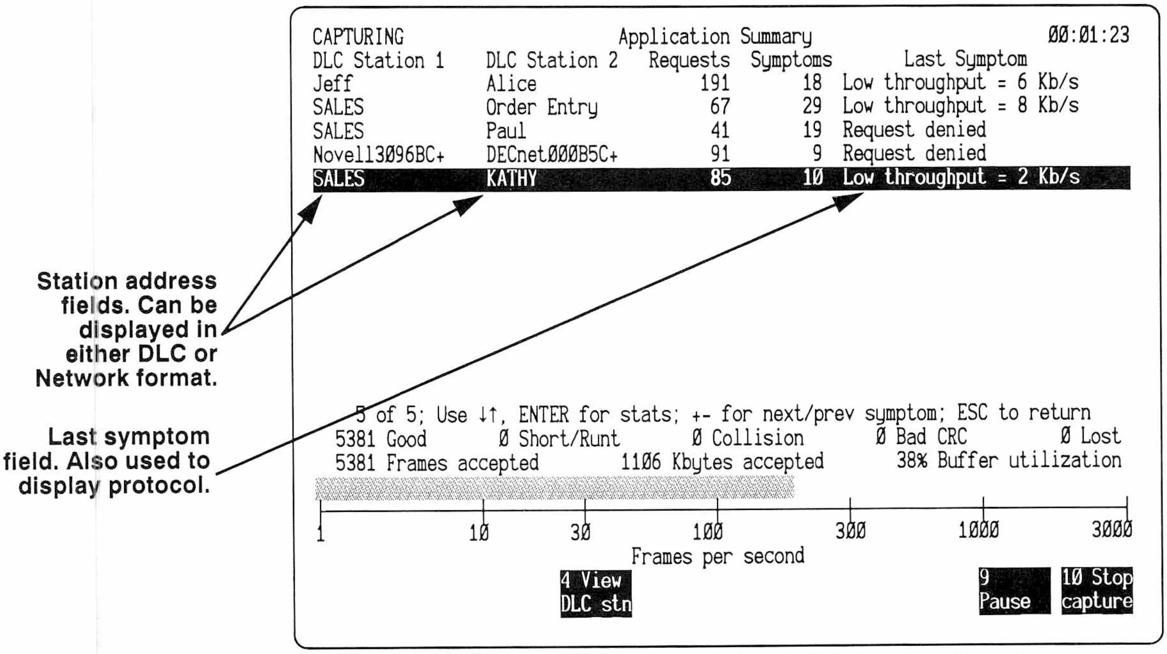
Notice that the Summary window lists the network addresses of the endpoints of each application layer connection detected by the analyzer. You can also view the connections in terms of the DLC addresses of the two endpoints. The display formats available for the Connection Summary window are exactly the same as those available at the Application layer. The only difference is that the Application Summary window counts application requests while the Connection Summary window counts the total number of frames transmitted on a connection. The available display formats for the Summary windows at the Application and Connection layers are summarized in Figure 4–29.

Shown in...	Format	Column Entries				
Figure 4–28	Net Station Format (default)	Net Station 1	Net Station 2	Requests Frames*	Symptoms	Last Symptom
Figure 4–30	DLC Station Format	DLC Station 1	DLC Station 2	Requests Frames*	Symptoms	Last Symptom
Figure 4–31	Protocol Format	Net Station 1	Net Station 2	Requests Frames*	Symptoms	Protocol

*The Frames counter appears in the Connection Summary window, while the Requests counter appears in the Application Summary window.

Figure 4–29. Application and Connection layer Summary window formats.

Figure 4–30 shows the Application Summary window in the DLC Station format.



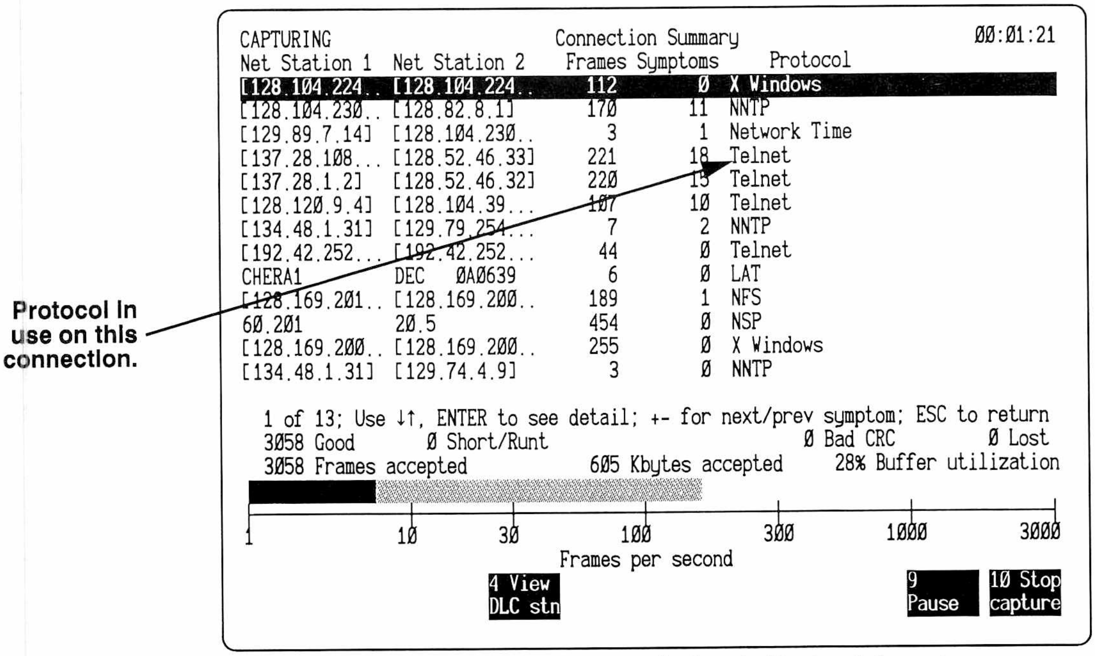
```
CAPTURING                    Application Summary                    ØØ:Ø1:23
DLC Station 1    DLC Station 2  Requests  Symptoms      Last Symptom
Jeff             Alice               191       18  Low throughput = 6 Kb/s
SALES            Order Entry          67       29  Low throughput = 8 Kb/s
SALES            Paul                 41       19  Request denied
Novell3Ø96BC+    DECnetØØØB5C+        91        9  Request denied
SALES            KATHY                85       1Ø  Low throughput = 2 Kb/s

  5 of 5; Use ↓↑, ENTER for stats; +- for next/prev symptom; ESC to return
  5381 Good        Ø Short/Runt      Ø Collision      Ø Bad CRC       Ø Lost
  5381 Frames accepted       11Ø6 Kbytes accepted      38% Buffer utilization
```

Station address fields. Can be displayed in either DLC or Network format.

Last symptom field. Also used to display protocol.

Figure 4–30. Application Summary window in DLC station format.

Figure 4–31 shows the Connection Summary window in the Protocol format.



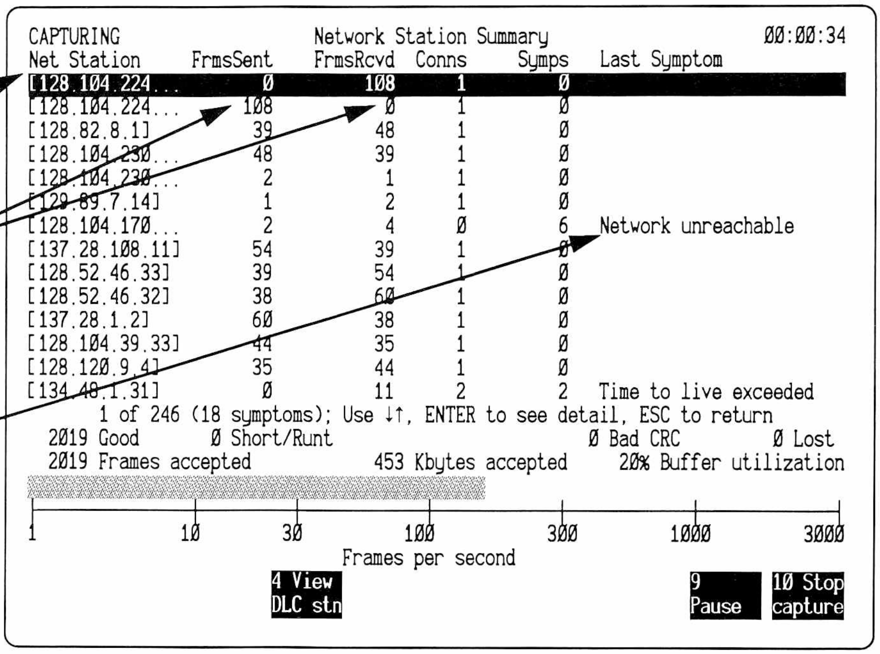
```
CAPTURING                       Connection Summary                 ØØ:Ø1:21
Net Station 1  Net Station 2   Frames Symptoms    Protocol
[128.1Ø4.224.. [128.1Ø4.224..    112        Ø  X Windows
[128.1Ø4.23Ø.. [128.82.8.1]      17Ø       11  NNTP
[129.89.7.14]  [128.1Ø4.23Ø..      3        1  Network Time
[137.28.1Ø8... [128.52.46.33]    221       18  Telnet
[137.28.1.2]   [128.52.46.32]    22Ø       15  Telnet
[128.12Ø.9.4]  [128.1Ø4.39...    1Ø7       1Ø  Telnet
[134.48.1.31]  [129.79.254...      7        2  NNTP
[192.42.252... [192.42.252...     44        Ø  Telnet
CHERA1         DEC    ØAØ639       6        Ø  LAT
[128.169.2Ø1.. [128.169.2ØØ..    189        1  NFS
6Ø.2Ø1         2Ø.5              454        Ø  NSP
[128.169.2ØØ.. [128.169.2ØØ..    255        Ø  X Windows
[134.48.1.31]  [129.74.4.9]        3        Ø  NNTP

  1 of 13; Use ↓↑, ENTER to see detail; +- for next/prev symptom; ESC to return
  3Ø58 Good        Ø Short/Runt                      Ø Bad CRC       Ø Lost
  3Ø58 Frames accepted            6Ø5 Kbytes accepted   28% Buffer utilization
```

Protocol in use on this connection.

Figure 4–31. Connection Summary window in Protocol format.

Network Station Summary Window

Figure 4–32 shows the default format for the Network Station Summary window. The information fields found in the Network Station Summary window are described beginning on page 4–38.



```
CAPTURING                  Network Station Summary                    ØØ:ØØ:34
Net Station      FrmsSent  FrmsRcvd  Conns     Symps  Last Symptom
[128.1Ø4.224...        Ø       1Ø8      1         Ø
[128.1Ø4.224...      1Ø8         Ø      1         Ø
[128.82.8.1]          39        48      1         Ø
[128.1Ø4.23Ø...       48        39      1         Ø
[128.1Ø4.23Ø...        2         1      1         Ø
[129.89.7.14]          1         2      1         Ø
[128.1Ø4.17Ø...        2         4      Ø         6  Network unreachable
[137.28.1Ø8.11]       54        39      1         Ø
[128.52.46.33]        39        54      1         Ø
[128.52.46.32]        38        6Ø      1         Ø
[137.28.1.2]          6Ø        38      1         Ø
[128.1Ø4.39.33]       44        35      1         Ø
[128.12Ø.9.4]         35        44      1         Ø
[134.48.1.31]          Ø        11      2         2  Time to live exceeded
     1 of 246 (18 symptoms); Use ↓↑, ENTER to see detail, ESC to return
  2Ø19 Good        Ø Short/Runt                     Ø Bad CRC          Ø Lost
  2Ø19 Frames accepted          453 Kbytes accepted     2Ø% Buffer utilization
```

Network Station addresses. Can also be viewed as DLC addresses.

Number of frames sent and received. Can also be viewed as bytes sent and received

Last symptom detected for this station. Can also be viewed as protocol in use.

Figure 4–32. Network Station Summary window.

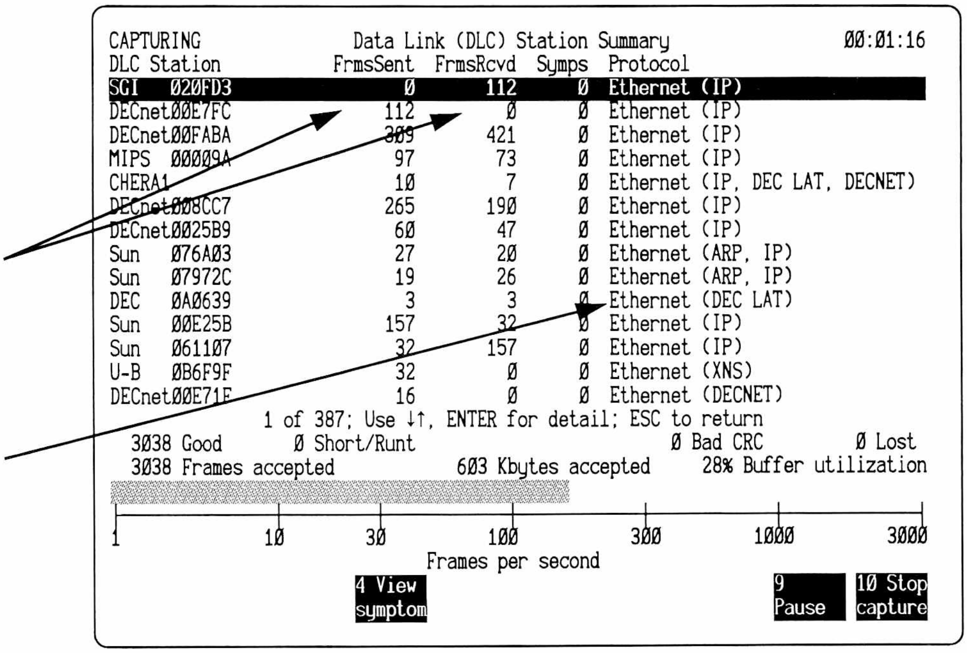
The available display formats for the Network Station Summary window are summarized in Figure 4–33.

Format	Column Entries					
Protocol Format	Net Station	Frames Sent	Frames Received	Connections	Symptoms	Protocol
Symptom Format	Net Station	Frames Sent	Frames Received	Connections	Symptoms	Last Symptom
DLC Station Format	DLC Station	Frames Sent	Frames Received	Connections	Symptoms	Last Symptom
Bytes Format	Net Station	Bytes Sent	Bytes Received	Connections	Symptoms	Last Symptom

Figure 4–33. Network Station layer Summary window formats.

DLC Station Summary Window

Figure 4–34 shows the Protocol display format for the DLC Station Summary window. The information fields found in the DLC Station Summary window are described beginning on page 4–38.



```
CAPTURING                 Data Link (DLC) Station Summary                 ØØ:Ø1:16
DLC Station                 FrmsSent  FrmsRcvd  Symps  Protocol
SGI    Ø2ØFD3                      Ø       112      Ø  Ethernet (IP)
DECnetØØE7FC                     112         Ø      Ø  Ethernet (IP)
DECnetØØFABA                     3Ø9       421      Ø  Ethernet (IP)
MIPS   ØØØØ9A                     97        73      Ø  Ethernet (IP)
CHERA1                            1Ø         7      Ø  Ethernet (IP, DEC LAT, DECNET)
DECnetØØ8CC7                     265       19Ø      Ø  Ethernet (IP)
DECnetØØ25B9                      6Ø        47      Ø  Ethernet (IP)
Sun    Ø76AØ3                     27        2Ø      Ø  Ethernet (ARP, IP)
Sun    Ø7972C                     19        26      Ø  Ethernet (ARP, IP)
DEC    ØAØ639                      3         3      Ø  Ethernet (DEC LAT)
Sun    ØØE25B                    157        32      Ø  Ethernet (IP)
Sun    Ø611Ø7                     32       157      Ø  Ethernet (IP)
U-B    ØB6F9F                     32         Ø      Ø  Ethernet (XNS)
DECnetØØE71E                      16         Ø      Ø  Ethernet (DECNET)
                     1 of 387; Use ↓↑, ENTER for detail; ESC to return
  3Ø38 Good          Ø Short/Runt                          Ø Bad CRC          Ø Lost
  3Ø38 Frames accepted              6Ø3 Kbytes accepted     28% Buffer utilization
```

Number of frames sent and received. Can also be viewed as bytes sent and received

Protocol in use (including physical topology). Can also be viewed as Last Symptom.

Figure 4–34. DLC Station Summary window.

The available display formats for the DLC Station Summary window are summarized in Figure 4–35.

Format	Column Entries				
Symptom Format	DLC Station	Frames Sent	Frames Received	Symptoms	Last Symptom
Bytes Format	DLC Station	Bytes Sent	Bytes Received	Symptoms	Last Symptom
Protocol Format	DLC Station	Frames Sent	Frames Received	Symptoms	Protocol

Figure 4–35. DLC Station Summary window formats

Subnet Pairs Summary Window

The Subnet Pairs Summary window lists all the pairs of communicating subnets detected by the Expert analyzer during its current capture session. The Expert analyzer learns about subnets by analyzing the information in the frames it captures. Symptoms are not categorized as occurring "at the subnet layer." The symptom counts in the Subnet Pairs Summary window refer to symptoms at all four Expert layers associated with the highlighted pair of subnets.

The Subnet Pairs Summary window (Figure 4–36) contains the following information:

Subnet 1 — A subnet which the Expert analyzer learned about from routing information embedded in frames. When the analyzer learns the symbolic name of the subnet, it will substitute it for the hex address.

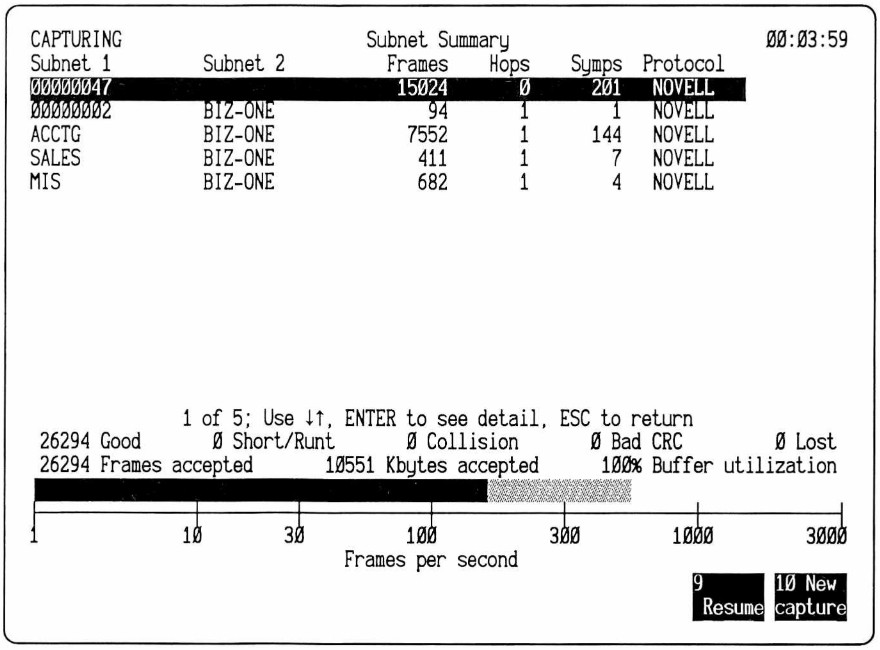
Subnet 2 — Often the address of the subnet to which the Expert analyzer is attached. The analyzer provides the subnet address.

Frames — If there is a pair of subnets listed, the Frames count measures the total number of frames that have been transmitted between the two subnets. If there is only one subnet listed (instead of a pair), then the Frames count describes the activity internal to that subnet.

Hops — The hop count between the two subnets. If the hop count is zero, it indicates either a local subnet or that no Routing Information Protocol (RIP) packets have been seen.

Symptoms — The total number of symptoms associated with traffic between these two subnets at the Expert Application and Connection layers. A subnet that has a high ratio of symptoms to packets is likely to have some kind of problem, or an area in which operation can be made more efficient.

Protocol — The protocol in use on Subnet 1.



```
CAPTURING                        Subnet Summary                         00:03:59
Subnet 1        Subnet 2           Frames   Hops    Symps  Protocol
00000047                            15024      0      201  NOVELL
00000002        BIZ-ONE                94      1        1  NOVELL
ACCTG           BIZ-ONE              7552      1      144  NOVELL
SALES           BIZ-ONE               411      1        7  NOVELL
MIS             BIZ-ONE               682      1        4  NOVELL



             1 of 5; Use ↓↑, ENTER to see detail, ESC to return
 26294 Good      0 Short/Runt      0 Collision      0 Bad CRC        0 Lost
 26294 Frames accepted      10551 Kbytes accepted      100% Buffer utilization
```

Figure 4–36. Subnet Pairs Summary window.

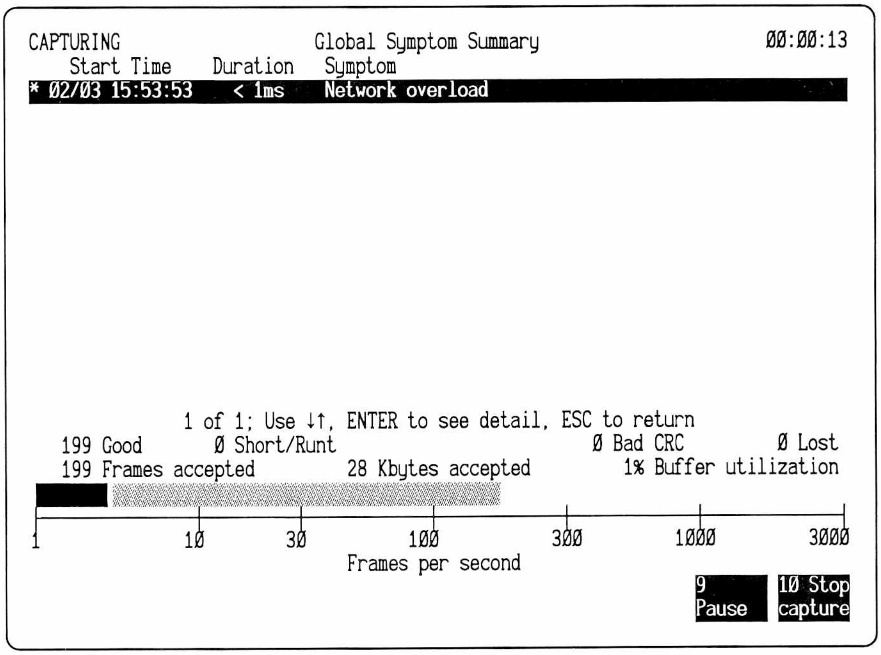
Global Symptom Summary Window

The Global Symptom Summary window provides information on global symptoms detected by the Expert analyzer during its current capture session.

Global symptoms include, but are not limited to:

- Network Overload
- Broadcast/Multicast Storm
- WAN Underload

Figure 4–37 shows the Global Symptom Summary window.



```
CAPTURING                    Global Symptom Summary                       ØØ:ØØ:13
    Start Time     Duration   Symptom
* Ø2/Ø3 15:53:53    < 1ms     Network overload

              1 of 1; Use ↓↑, ENTER to see detail, ESC to return
   199 Good        Ø Short/Runt                        Ø Bad CRC          Ø Lost
   199 Frames accepted        28 Kbytes accepted          1% Buffer utilization

1              1Ø        3Ø          1ØØ          3ØØ         1ØØØ         3ØØØ
                                Frames per second
```

Figure 4–37. Global Symptom Summary window.

The Global Symptom Summary window contains the following information:

Start Time — The time and date at which the symptom was first detected by the analyzer.

Duration — The length of time (in milliseconds) during which the symptom was valid.

If there is an asterisk in the far left column, as in Figure 4–37, the symptom is still active.

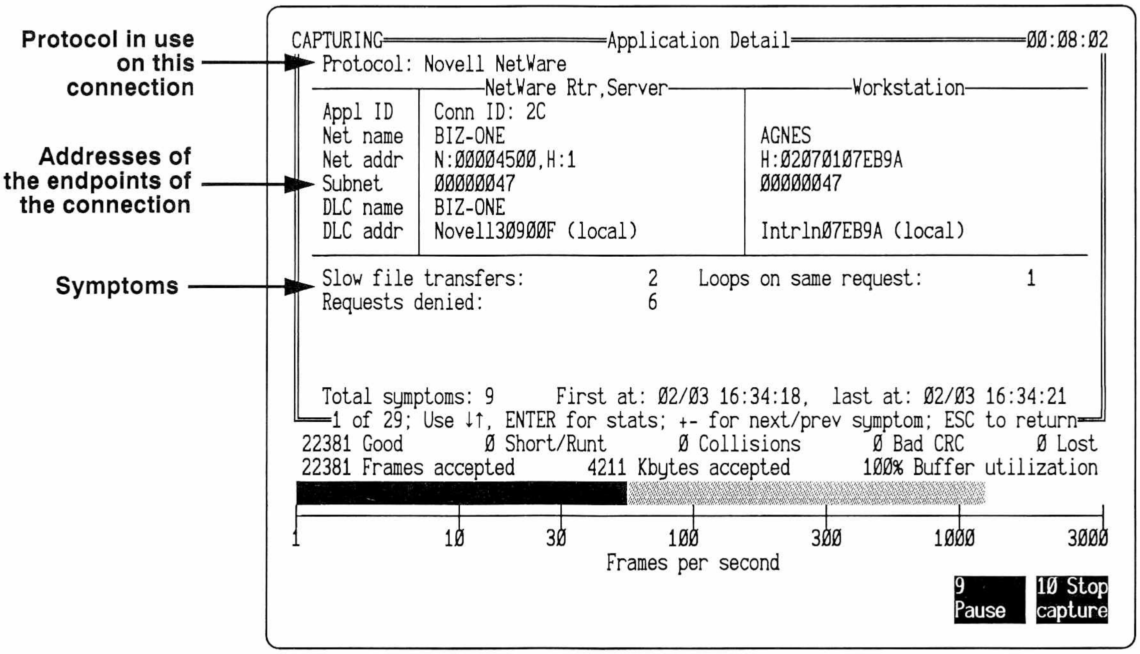
Symptom — A one-line description of the symptom detected.

You can control when the analyzer generates Network Overload symptoms and diagnoses by setting the **LAN Overload** and **LAN Overload %** thresholds in the **Expert Settings\Thresholds\DLC Station** menu. Similarly, WAN Overload symptoms and diagnoses are controlled by the **WAN Overload Timer** and

WAN Overload % thresholds. Broadcast/Multicast storm symptoms and diagnoses are controlled by the **Broadcast sy** and **Broadcast dg** thresholds. For information on Expert thresholds, refer to "Setting Thresholds for Symptoms and Diagnoses" on page 3–13.

Symptom and Network Object Detail Windows

The Symptom and Network Object Detail windows provide specific information about particular connections, network stations, or DLC stations. Figure 4–38 shows the Detail window for a connection between the NetWare server BIZ-ONE and the workstation AGNES at the Application layer. The analyzer provides the DLC and network addresses of the endpoints of the connection, the protocol in use, and a list of all the symptoms associated with this connection. At this point, you would probably pause capture by pressing F9 (**Pause**), and press F1 (**Explain**) to read the context-sensitive Explain message associated with these symptoms.


Protocol in use on this connection
Addresses of the endpoints of the connection
Symptoms
9 Pause
10 Stop capture

```
CAPTURING════════════════════Application Detail══════════════════════00:08:02
  Protocol: Novell NetWare
  ──────────────NetWare Rtr,Server──────────────────────Workstation─────────
  Appl ID   Conn ID: 2C
  Net name  BIZ-ONE                             AGNES
  Net addr  N:00004500,H:1                      H:02070107EB9A
  Subnet    00000047                            00000047
  DLC name  BIZ-ONE
  DLC addr  Novell30900F (local)                Intrln07EB9A (local)
  ───────────────────────────────────────────────────────────────────────
  Slow file transfers:            2   Loops on same request:           1
  Requests denied:                6



  Total symptoms: 9      First at: 02/03 16:34:18,  last at: 02/03 16:34:21
═1 of 29; Use ↓↑, ENTER for stats; +- for next/prev symptom; ESC to return═
22381 Good          0 Short/Runt       0 Collisions        0 Bad CRC      0 Lost
22381 Frames accepted        4211 Kbytes accepted        100% Buffer utilization

1           10       30        100          300        1000        3000
                            Frames per second
```

Figure 4–38. Application Detail window.

Displaying the Detail Window

There are two ways to display the Detail window:

- From the Symptom and Network Object column of the Expert Overview
- From the Diagnoses column of the Expert Overview

To display a Detail window from the Symptom and Network Object column of the Expert Overview:

1. In the Symptom and Network Object column, use the cursor keys to highlight the Expert layer containing the connection, network station, or DLC station in which you are interested.
2. Press Enter.

   Result: The Summary window for the selected Expert layer appears.
3. Use the cursor keys to highlight the desired connection, network station, or DLC station in the Summary window.
4. Press Enter.

   Result: A Detail window similar to Figure 4–38 appears. The exact format of the Detail window depends on the layer selected and the number of symptoms detected.

You can also display a Symptom and Network Object Detail window from the Diagnoses column of the Expert Overview.

To display a Symptom and Network Object Detail window from the Diagnoses column of the Expert Overview:

1. In the Diagnoses column of the Expert Overview, use the cursor keys to highlight an Expert layer containing at least one diagnosis.
2. Press Enter.

   Result: The Diagnosis Summary for the selected layer appears.
3. Use the cursor keys to highlight the desired diagnosis and press Enter.

   Result: The Diagnosis Detail window appears.

   Note: The Diagnosis Detail window is different from the Symptom and Network Object Detail window. The Diagnosis Detail window provides specific information on a diagnosis, while the Detail window provides more general information such as network addresses, DLC addresses, and symptoms detected.
4. Press Enter.

   Result: The Detail window for the connection, network station, or DLC station associated with the selected diagnosis appears. Figure 4–38 is an example of a Detail window.

   Note: From the Diagnoses column of the Expert Overview, you cannot display the Subnet Pairs or the Global Symptom Detail windows. These windows can only be displayed from the Symptom and Network Object column of the Expert Overview.

Note: From the Symptom and Network Object column of the Expert Overview, you can use the cursor keys to scroll through the Detail windows for each connection, network station, or DLC station listed in the Summary display (from the Diagnoses column of the Expert Overview, you cannot). When you return to the Summary window from the Detail windows, the analyzer will automatically highlight the connection or address associated with the Detail display from which you came.

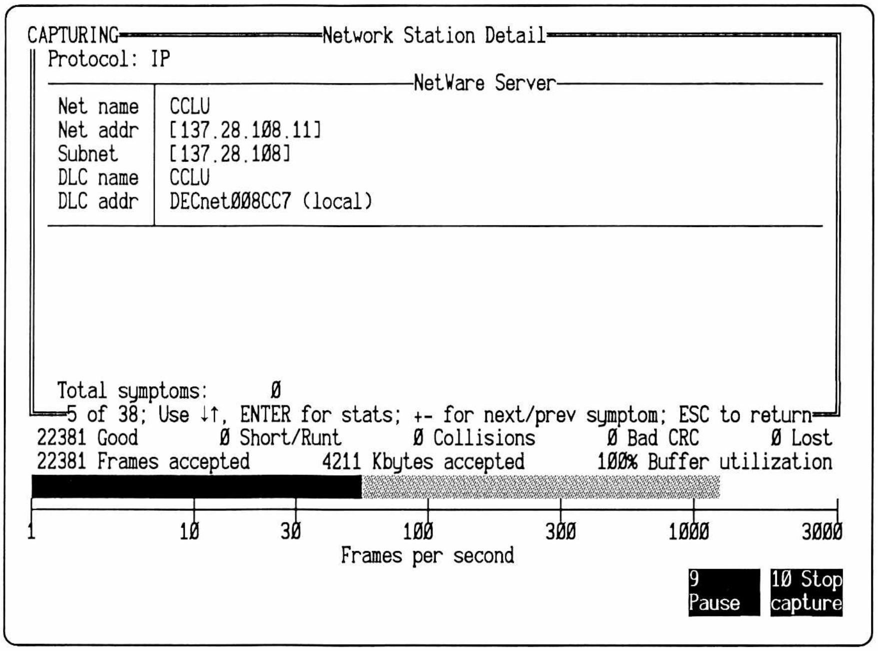
Figure 4–1 on page 4–4 summarizes the relationships between the various Expert windows.

Information in the Detail Windows

The information presented in the Detail windows is very similar at each of the four Expert layers. However, the Subnet Pairs and Global Symptom Detail windows are somewhat different. Those windows are described in later sections.

The Detail windows for the Network Station and DLC layers will contain less information than those at the Application and Connection layers. This is because the analyzer detects information for single stations at the Network Station and DLC layers, while at the Application and Connection layers it detects information about connections between two stations. This means that there is twice as much address information to present in the Detail window.

Figure 4–39 is an example of a Detail window at the Network Station layer. Notice that the information presented is the same as in Figure 4–38 but for only one station.



```
CAPTURING────────────────Network Station Detail──────────────────────
 Protocol: IP
 ─────────────────────────NetWare Server─────────────────────────
  Net name │ CCLU
  Net addr │ [137.28.108.11]
  Subnet   │ [137.28.108]
  DLC name │ CCLU
  DLC addr │ DECnet008CC7 (local)
 ────────────────────────────────────────────────────────────────



  Total symptoms:      0
══5 of 38; Use ↓↑, ENTER for stats; +- for next/prev symptom; ESC to return══
22381 Good          0 Short/Runt       0 Collisions        0 Bad CRC        0 Lost
22381 Frames accepted        4211 Kbytes accepted        100% Buffer utilization
```

Figure 4–39. Network Station Detail window.

The list below summarizes the information found in the Detail windows. Not all the information is found in every screen. The exact information in the Detail display depends on the Expert layer and the object highlighted.

Protocol

The protocol in use on this connection. If the analyzer does not recognize the protocol in use, it will substitute the well-know port name (which is usually also a protocol name, such as Telnet or FTP).

Appl ID

The application ID for this connection. Most protocols use an identification scheme to give unique names to connections between network stations. The Expert analyzer learns the identification scheme for the particular protocol involved and displays that information.

For example, TCP uses Port numbers, DECnet uses Logical link numbers, and Novell uses Connection IDs. The Expert analyzer displays the identification scheme appropriate to the protocol in use.

Net name

The symbolic name for this station. This field will remain blank until the analyzer learns the symbolic name.

Net addr

The network address of this station.

subnet

The subnet on which this station resides.

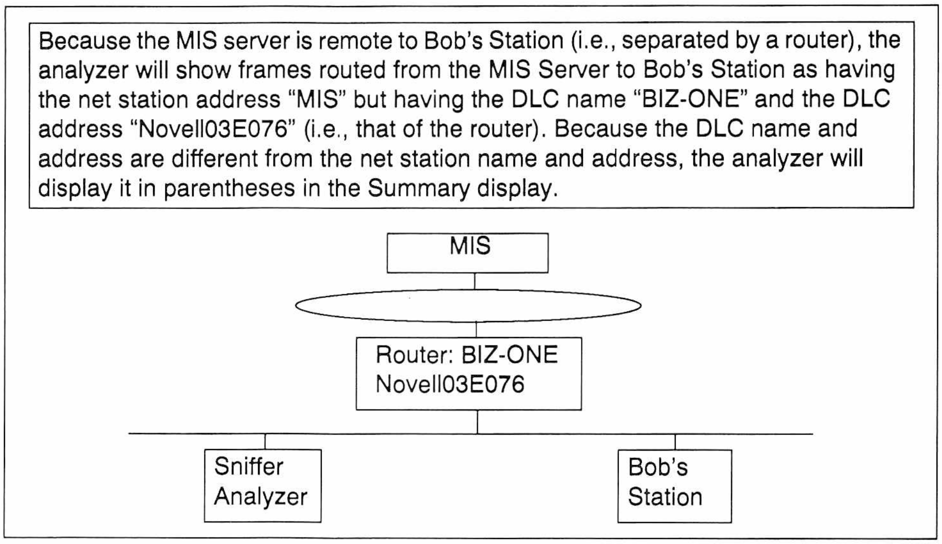
DLC name

The symbolic DLC name for this station. This field will remain blank until the analyzer learns the symbolic name.

DLC addr

The DLC address for this station. The analyzer automatically attempts to interpret the first three bytes of the address as the name of the NIC's manufacturer. When it is able to find the manufacturer's code in its table of manufacturers, the analyzer replaces the first three bytes of the station address with an ASCII abbreviation of the manufacturer's name.

The DLC address of a station may be different than the network station address. This occurs when the analyzer captures frames from a remote station. The analyzer will show the DLC address of the router rather than that of the originating station. When this occurs, the DLC address will be followed by the message `(remote routed)`. Figure 4–40 shows how this can happen.



Because the MIS server is remote to Bob's Station (i.e., separated by a router), the analyzer will show frames routed from the MIS Server to Bob's Station as having the net station address "MIS" but having the DLC name "BIZ-ONE" and the DLC address "Novell03E076" (i.e., that of the router). Because the DLC name and address are different from the net station name and address, the analyzer will display it in parentheses in the Summary display.

Figure 4–40. How the analyzer interprets the DLC name and address of remote stations.

Total symptoms — Total number of symptoms associated with this connection or station. The Detail window also lists each symptom associated with the selected connection or station, followed by a dynamic counter.

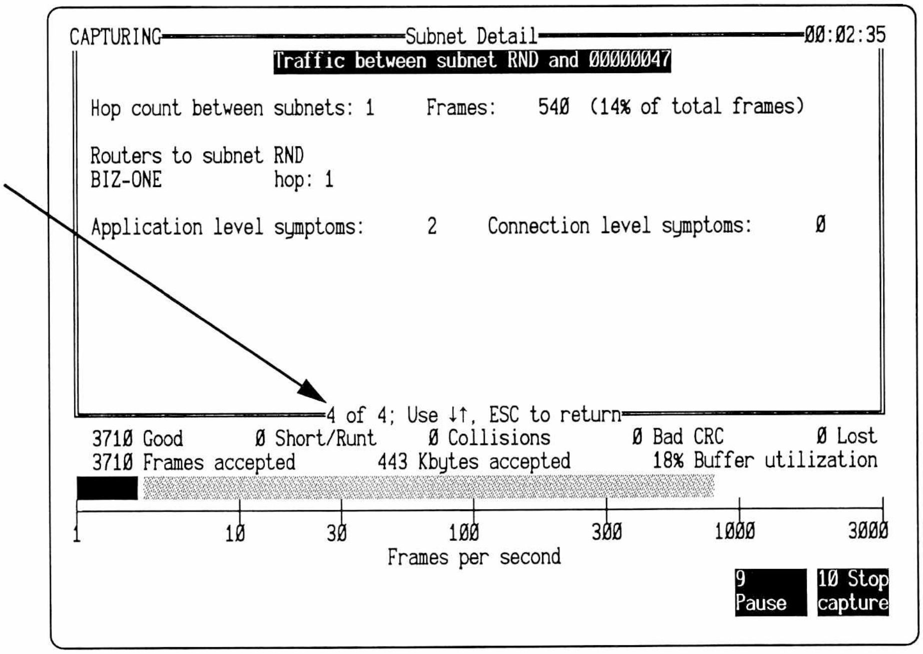
Detail windows will often include a short message about a particular symptom detected by the analyzer. For more information on these messages, press F1 (**Explain**) to invoke the Explain message pertinent to the current display.

Subnet Pairs Detail Window

The Subnet Pairs Detail window displays the number of packets transferred between two subnets and the number of symptoms (at the Connection and Application Expert layers) associated with those packets. The symptoms are presented with an individual counter for each Expert layer.

Additionally, the Detail window lists any routers used to access the subnet on which the Expert analyzer is not attached. The hop count is included. Figure 4–41 is an example of a Subnet Pairs Detail window.

You can scroll through the Detail windows for all subnets detected by the analyzer.



```
CAPTURING─────────────────Subnet Detail──────────────────00:02:35
              Traffic between subnet RND and 00000047

 Hop count between subnets: 1     Frames:    540  (14% of total frames)

 Routers to subnet RND
 BIZ-ONE           hop: 1

 Application level symptoms:      2     Connection level symptoms:      0



─────────────────────4 of 4; Use ↓↑, ESC to return──────────────────
 3710 Good        0 Short/Runt     0 Collisions        0 Bad CRC          0 Lost
 3710 Frames accepted       443 Kbytes accepted       18% Buffer utilization

1          10      30        100         300        1000        3000
                          Frames per second
```

Figure 4–41. Subnet Pairs Detail Window.

The list below describes the information in the Subnet Detail window:

Hop count between subnets — Lists the number of hops between these two subnets.

Frames — Lists the number of frames exchanged at the Expert Connection layer. The **% of total frames** counter is the ratio between the number of frames exchanged at the Expert Connection layer and the total number of frames exchanged at all layers. This gives you an idea of the "useful" traffic on your network.

Routers to subnet — Lists the routers used to access the subnet.

Symptoms — Lists the number of symptoms detected at the Application and Connection Expert layers.

The information in the Subnet Pairs Detail window varies according to the protocol in use. For example, Figure 4–41 shows the Subnet Pairs Detail window for a pair of communicating Novell subnets. The Subnet Pairs Detail window for a DECnet network includes protocol-specific information, such as DECnet areas. TCP/IP Subnet Pairs Detail windows are similar to the Novell window. However, you should be aware of how to define the subnet mask for the various TCP/IP networks to which you will attach the Expert analyzer. See "Setting Subnet Masks" on page 3–7 for more information on defining the subnet mask.

You display the Subnet Pairs Detail window in the same way you display any Detail window. See "To display a Summary window at any of the Expert layers:" on page 4–37.

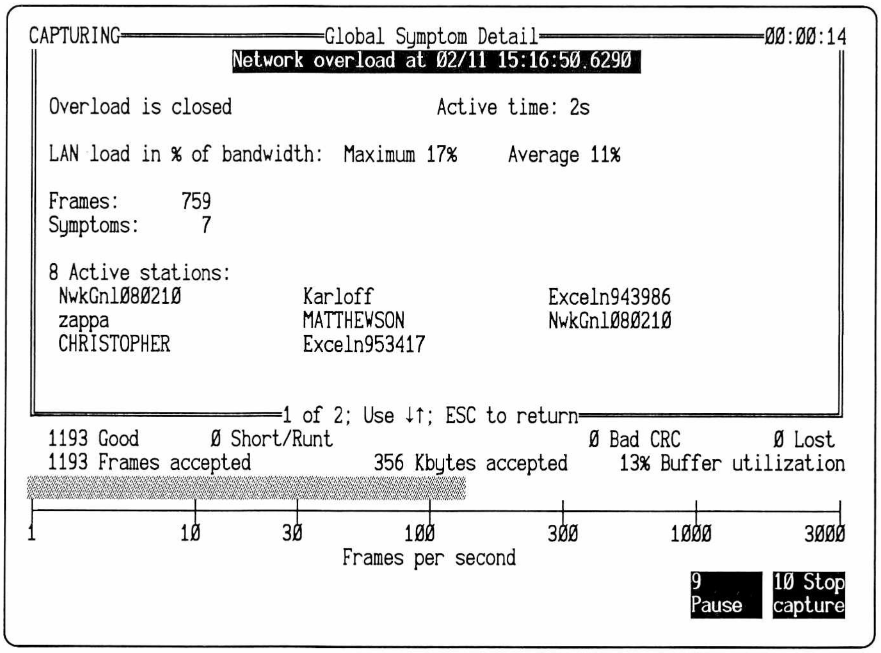
Note: One of the entries in the Subnet Summary window will not list a pair of communicating subnets. That is the entry for the subnet to which the Sniffer Network Analyzer is attached. Its Detail window will measure frames and symptoms for its specific subnet alone.

Global Symptom Detail Window

The Global Symptom Detail window provides specific information on certain global symptoms. Global symptoms include:

- LAN Overload
- Broadcast/Multicast Storm
- WAN Overload
- WAN Underload

You can control when these symptoms are generated by adjusting the Expert thresholds. For more information on Expert thresholds, see "Setting Thresholds for Symptoms and Diagnoses" on page 3–13.



```
CAPTURING═══════════════Global Symptom Detail════════════════ØØ:ØØ:14
                  Network overload at Ø2/11 15:16:5Ø.629Ø

 Overload is closed                    Active time: 2s

 LAN load in % of bandwidth:  Maximum 17%     Average 11%

 Frames:       759
 Symptoms:       7

 8 Active stations:
  NwkGnlØ8Ø21Ø            Karloff                 Exceln943986
  zappa                   MATTHEWSON              NwkGnlØ8Ø21Ø
  CHRISTOPHER             Exceln953417

════════════════════════1 of 2; Use ↓↑; ESC to return═════════════════
 1193 Good       Ø Short/Runt                     Ø Bad CRC       Ø Lost
 1193 Frames accepted        356 Kbytes accepted    13% Buffer utilization
```

Figure 4–42. Global Symptom Detail window.

The Global Symptom Detail window (Figure 4–42) is displayed in the same way you display any Detail window. See "To display a Summary window at any of the Expert layers:" on page 4–37.

Information in the Global Symptom Detail Window

The list below summarizes the information found in the Global Symptom Detail Window:

Active time
Length of time for which the LAN Overload or Broadcast/Multicast storm symptom was active.

State
Current status of the named symptom. Status is either closed or active.

Max load %
Maximum network load during the time the named symptom was active. Measured as a percentage of available bandwidth, where available bandwidth is the theoretical maximum of the medium in use (for example, 10 Mbps is the theoretical maximum for Ethernet).

Average load %
Average network load during the time the named symptom was active. Measured as percentage of available bandwidth (see **Max load %**, above).

Broadcasts
Number of broadcast frames detected.

Active stations
Number of active stations transmitting during the time the LAN Overload or Broadcast\Multicast storm symptom was active. The stations are listed by address or symbolic name.

Frames
Total number of frames associated with the highlighted overload.

Symptoms
Total number of symptoms associated with frames associated with highlighted overload.

Symptom and Network Object Statistics Windows

Statistics windows provide in-depth statistics relating to a selected application, connection, network station, or DLC station. Statistics windows provide information on topics such as average file performance, number of frames sent, and the number of connections for a given station. The exact information depends on the layer for which the Statistics window is displayed and the protocol in use.

The following sections describe the Statistics windows for each of the following Expert layers:

- Application
- Connection
- Network Station
- DLC Station

Note: There are no Statistics windows associated with the Subnet Pairs or Global Symptom screens.

Displaying a Statistics Window

There are two ways to display a Statistics window:

- From the Symptom and Network Object column of the Expert Overview
- From the Diagnoses column of the Expert Overview

To display a Statistics window from the Symptom and Network Object column of the Expert Overview:

1. In the Symptom and Network Object column of the Expert Overview, display the Summary window for the Expert layer containing the connection, network station or DLC station in which you are interested.
2. From the Summary window, display the Detail window for the desired connection, network station, or DLC station.
3. Press Enter.

   Result: A Statistics window similar to Figure 4–43 appears. The exact format of the Statistics window depends on the layer selected, the protocol in use, and the number of symptoms detected.

You can also display a Statistics window from the Diagnoses column of the Expert Overview.

To display a Statistics window from the Diagnoses column of the Expert Overview:

1. In the Diagnoses column of the Expert Overview, use the cursor keys to highlight an Expert layer containing at least one diagnosis.
2. Press Enter.

   Result: The Diagnosis Summary for the selected layer appears.
3. Use the cursor keys to highlight the desired diagnosis and press Enter.

   Result: The Diagnosis Detail window appears.
4. Press Enter.

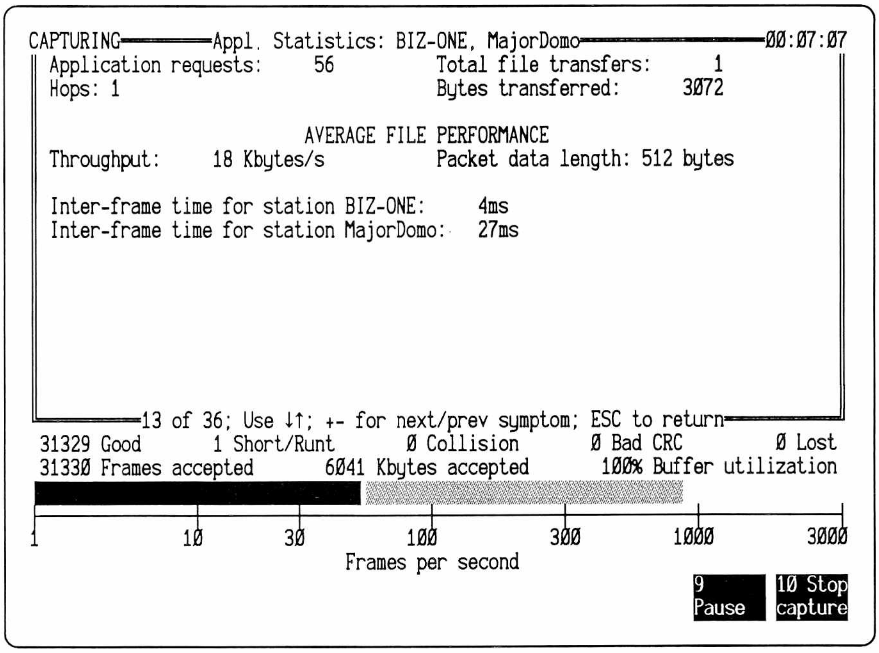
   Result: The Detail window associated with the selected diagnosis appears. (This Detail window is different from the Diagnosis Detail window.)
5. Press Enter.

   Result: The Statistics window associated with the selected diagnosis appears. Figure 4–43 shows a Statistics window at the Application layer.

Figure 4–1 on page 4–4 summarizes the relationships between the various Expert windows.

Application Statistics Window

The Application Statistics window provides statistics related to specific connections detected at the Application layer. Figure 4–43 is an example of the Statistics window for an Application layer connection between the server BIZ-ONE and the workstation MajorDomo.



```
CAPTURING═══════Appl. Statistics: BIZ-ONE, MajorDomo═══════════════ØØ:Ø7:Ø7
 Application requests:    56          Total file transfers:     1
 Hops: 1                              Bytes transferred:      3Ø72

                         AVERAGE FILE PERFORMANCE
 Throughput:      18 Kbytes/s         Packet data length: 512 bytes

 Inter-frame time for station BIZ-ONE:       4ms
 Inter-frame time for station MajorDomo:     27ms

══════════13 of 36; Use ↓↑; +- for next/prev symptom; ESC to return══════════
 31329 Good        1 Short/Runt        Ø Collision        Ø Bad CRC        Ø Lost
 3133Ø Frames accepted      6Ø41 Kbytes accepted      1ØØ% Buffer utilization
```

Figure 4–43. Application Statistics window.

The Application Statistics window provides the following statistics:

Application requests — The number of file requests detected for this connection.

Total file transfers — The number of files transferred on this connection.

Hops — The number of hops between the endpoints of this connection.

Bytes transferred — The number of bytes transferred on this connection.

If the analyzer has detected at least one file transferred on a given connection, the Statistics window will also contain statistics on average file performance. Average file performance statistics include:

Throughput — Measures the average speed at which data was transferred between the two stations. Units are in Kbytes/s.

Packet data length — Average length of data packets on this connection. Units are in bytes.

Interframe time for station	Average response time for a given station. With a request/reply protocol such as Novell PEP, the Interframe time is simply the average of the delta times between when a station receives a request and when it sends a reply. In a windowing protocol, such as TCP/IP, or DECnet, the Interframe time is the average of both the delta time between when a station receives a request and sends a reply and the delta times between replies to a single file request. Figure 4–44 summarizes how Interframe time is calculated for both types of protocols.

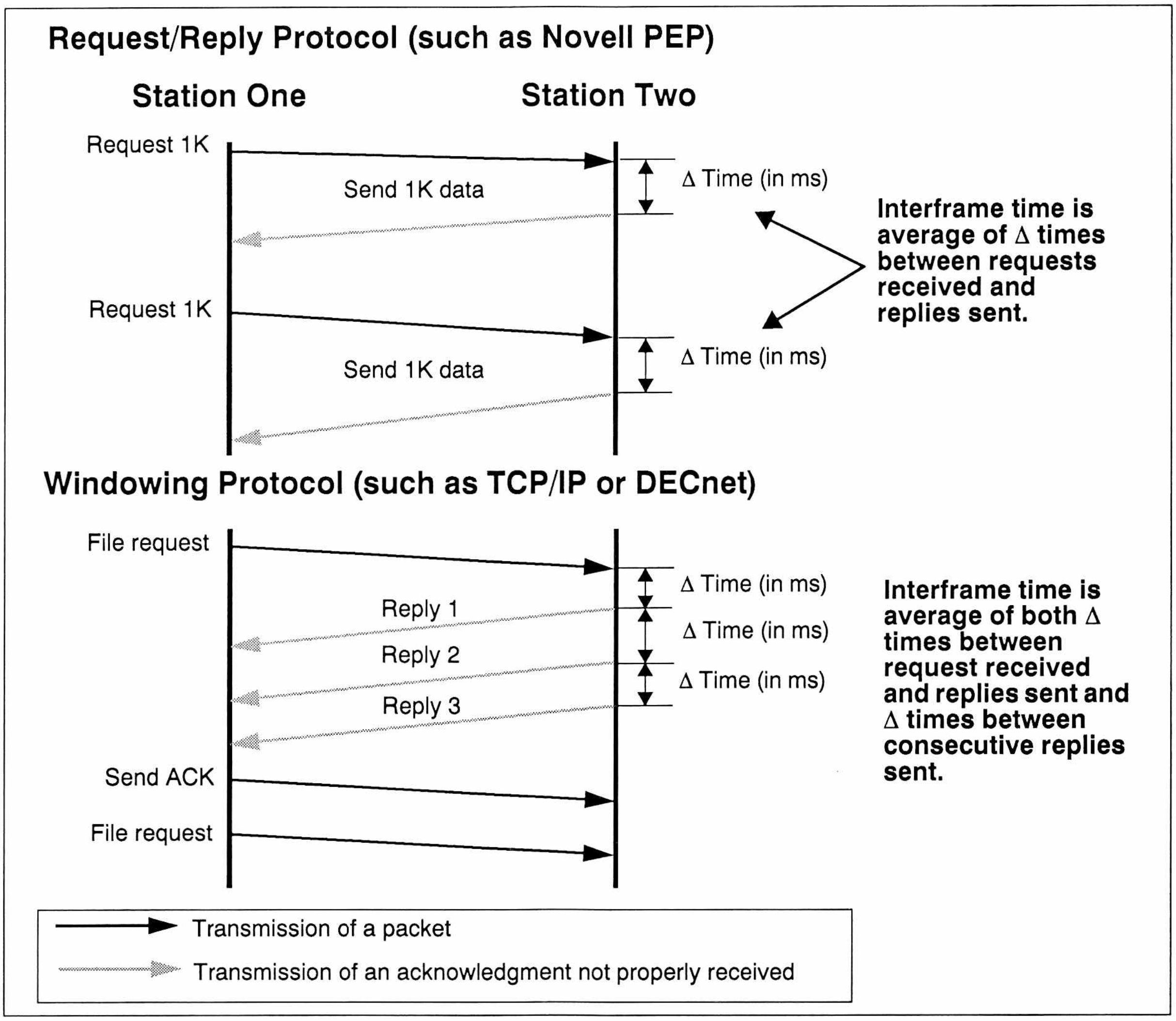
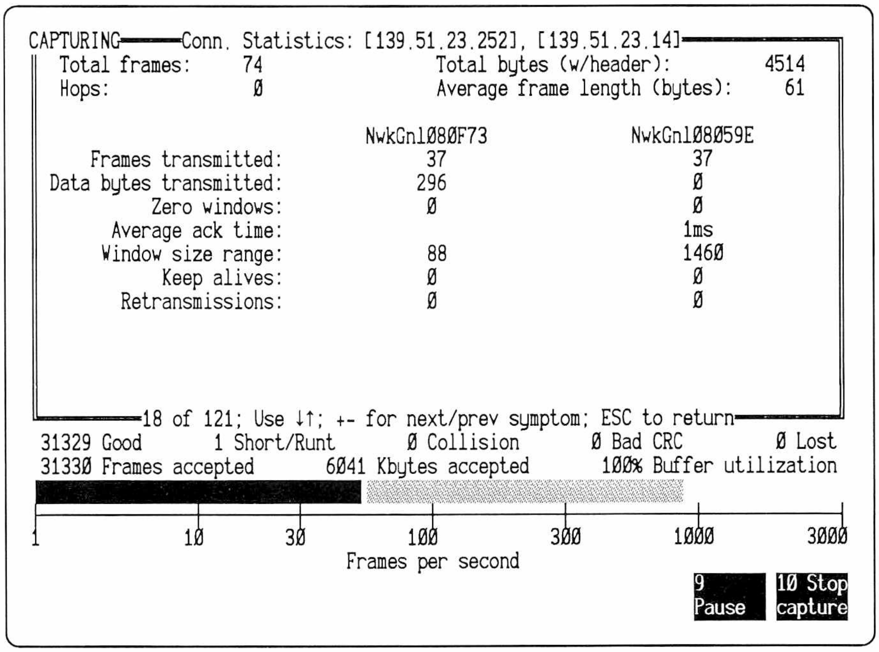

Request/Reply Protocol (such as Novell PEP)
Station One
Station Two
Request 1K
Send 1K data
Δ Time (in ms)
Interframe time is average of Δ times between requests received and replies sent.
Request 1K
Send 1K data
Δ Time (in ms)
Windowing Protocol (such as TCP/IP or DECnet)
File request
Reply 1
Reply 2
Reply 3
Δ Time (in ms)
Δ Time (in ms)
Δ Time (in ms)
Interframe time is average of both Δ times between request received and replies sent and Δ times between consecutive replies sent.
Send ACK
File request
Transmission of a packet
Transmission of an acknowledgment not properly received

Figure 4–44. How the Expert analyzer calculates the value for Interframe time.

Connection Statistics Window

The Connection Statistics window provides information on specific connections detected at the Connections layer. The exact information in the Statistics window depends on the protocol in use. Figure 4–45 is an example of the Statistics window for a connection using the TCP/IP protocol.



```
CAPTURING——Conn. Statistics: [139.51.23.252], [139.51.23.14]
  Total frames:      74              Total bytes (w/header):         4514
  Hops:              Ø               Average frame length (bytes):     61

                                NwkGnlØ8ØF73               NwkGnlØ8Ø59E
    Frames transmitted:             37                         37
  Data bytes transmitted:           296                        Ø
          Zero windows:             Ø                          Ø
       Average ack time:                                       1ms
      Window size range:            88                         146Ø
            Keep alives:            Ø                          Ø
        Retransmissions:            Ø                          Ø

——18 of 121; Use ↓↑; +- for next/prev symptom; ESC to return——
 31329 Good       1 Short/Runt      Ø Collision     Ø Bad CRC       Ø Lost
 3133Ø Frames accepted    6Ø41 Kbytes accepted    1ØØ% Buffer utilization
```

Figure 4–45. Connection Statistics window (in this case, for TCP/IP).

The following information is found in the Connection Statistics window regardless of the protocol used:

Total frames — Total number of frames transmitted on this connection.

Total bytes — Total number of bytes transferred on this connection. This number includes the headers of all frames transmitted.

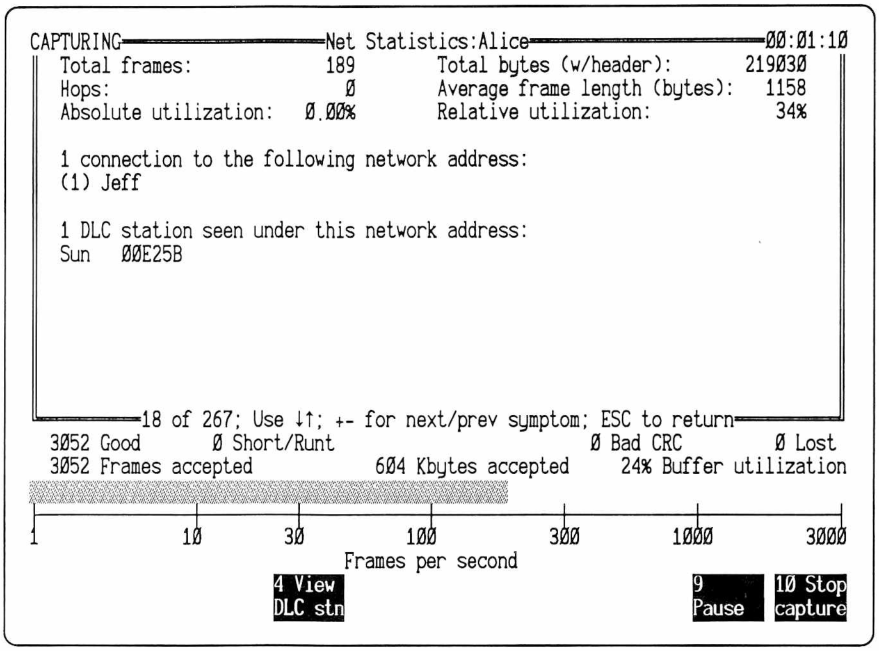
Hops — The number of hops between the endpoints of this connection.

Average frame length — The average length of the frames transmitted on this connection. Units are in bytes.

The Connection Statistics window also provides protocol-specific statistics. Figure 4–45 shows the statistics provided for a TCP/IP connection.

Network Station Statistics Window

The Network Station Statistics window provides statistics for individual network stations. Notice that the counters in Figure 4–46 are the same as those in the Connection Statistics window in Figure 4–45. However, in the Network Station window, these counters pertain to the highlighted station alone, rather than a connection. The list below summarizes the information found in the Network Station Statistics window.



```
CAPTURING═══════════════════Net Statistics:Alice═══════════════════════ØØ:Ø1:1Ø
   Total frames:              189       Total bytes (w/header):       219Ø3Ø
   Hops:                        Ø       Average frame length (bytes):  1158
   Absolute utilization:    Ø.ØØ%       Relative utilization:           34%

   1 connection to the following network address:
   (1) Jeff

   1 DLC station seen under this network address:
   Sun   ØØE25B

═══════════18 of 267; Use ↓↑; +- for next/prev symptom; ESC to return══════════
  3Ø52 Good       Ø Short/Runt                     Ø Bad CRC         Ø Lost
  3Ø52 Frames accepted          6Ø4 Kbytes accepted     24% Buffer utilization
```

Figure 4–46. Network Station Statistics window.

Total frames	Total number of frames transmitted and received by this station.
Total bytes	Total number of bytes transmitted and received by this station. This number includes the headers of all frames.
Hops	Total number of hops associated with frames sent and received by this station.
Average frame length	The average length of all frames transmitted and received by this station. Units are in bytes.
Absolute utilization	Network utilization for this DLC station computed as a percentage of maximum theoretical available bandwidth. For example, the theoretical maximum available bandwidth for Ethernet is 10 Mbps. Absolute utilization is updated every second and is measured over the time period since the first frame of the current capture session was passed into the capture buffer.

Relative utilization

Network utilization for this DLC station computed as a percentage of traffic seen by the analyzer. For example, if the analyzer has seen 100 bytes of traffic and Station A has sent 50 of them, then Station A's relative utilization is 50 percent.

Connections to net stations

The Statistics window lists all DLC stations to which the highlighted station has connected, as well as a counter of how many times.

In Figure 4–46, the network station Alice has connected to the DLC station Jeff once.

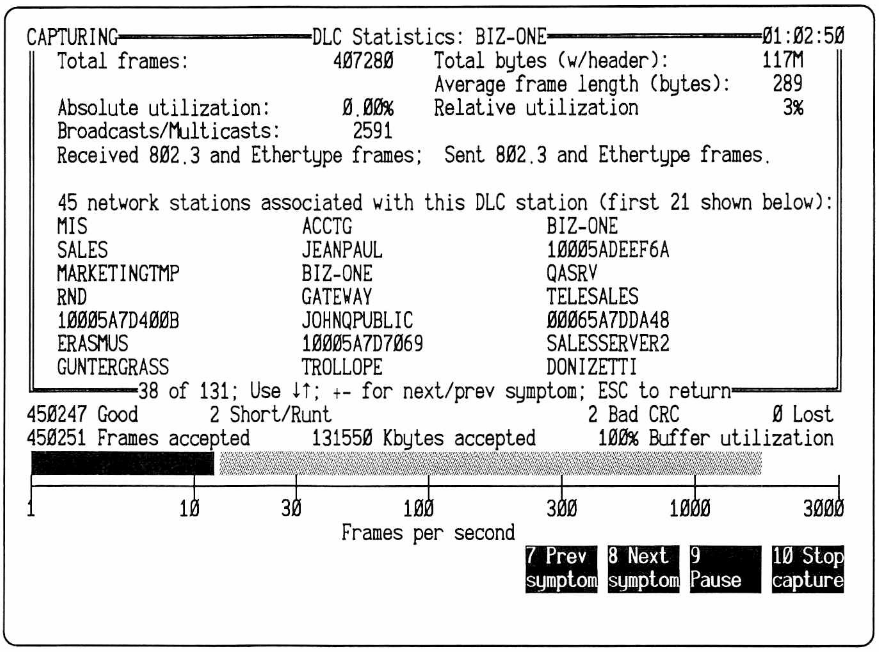
Associated DLC addresses

The Statistics window provides the DLC addresses of stations associated with the selected network station (see below).

If frames have been routed from a remote network segment, the two stations may not be the same. In that case, the associated DLC station would probably be the router or server through which the frames were routed. If this is the case, the hop count will be greater than one, indicating that frames have been remote routed. Then, the DLC station address will probably be different from the network station address.

DLC Station Statistics Window

Just as the Network Station Statistics window provides statistics for network stations, the DLC Station Statistics window provides statistics for DLC stations. Figure 4–47 shows the DLC Station Statistics window for the DLC station BIZ-ONE.



```
CAPTURING════════════════DLC Statistics: BIZ-ONE══════════════════01:02:50
   Total frames:             407280    Total bytes (w/header):        117M
                                       Average frame length (bytes):   289
   Absolute utilization:      0.00%    Relative utilization             3%
   Broadcasts/Multicasts:      2591
   Received 802.3 and Ethertype frames;  Sent 802.3 and Ethertype frames.

   45 network stations associated with this DLC station (first 21 shown below):
   MIS                    ACCTG                  BIZ-ONE
   SALES                  JEANPAUL               10005ADEEF6A
   MARKETINGTMP           BIZ-ONE                QASRV
   RND                    GATEWAY                TELESALES
   10005A7D400B           JOHNQPUBLIC            00065A7DDA48
   ERASMUS                10005A7D7069           SALESSERVER2
   GUNTERGRASS            TROLLOPE               DONIZETTI
═════════38 of 131; Use ↓↑; +- for next/prev symptom; ESC to return══════════
450247 Good        2 Short/Runt                    2 Bad CRC          0 Lost
450251 Frames accepted     131550 Kbytes accepted     100% Buffer utilization
```

Figure 4–47. DLC Station Statistics Window.

The DLC Station Statistics window is very similar to the Network Station Statistics window, inasmuch as it contains several of the same counters. These counters include:

- Total frames
- Total bytes
- Average frame length

However, the DLC Station Statistics window also provides the following information:

Absolute utilization

Network utilization for this DLC station computed as a percentage of maximum theoretical available bandwidth. For example, the theoretical maximum available bandwidth for Ethernet is 10 Mbps.

Absolute utilization is updated every second and is measured over the time period since the first frame of the current capture session was passed into the capture buffer.

Broadcasts/Multicasts

Number of broadcast/multicast frames sent and received.

Received/Sent

On an Ethernet network, the Statistics window describes the type of Ethernet frames sent and received by the highlighted station. In Figure 4–47, the DLC station, "BIZ-ONE," sent and received 802.3 and other Ethertype frames.

Relative utilization

Network utilization for this DLC station computed as a percentage of traffic seen by the analyzer. For example, if the analyzer has seen 100 bytes of traffic and Station A has sent 50 of them, then Station A's relative utilization is 50 percent.

Associated network stations

This field lists up to the first 21 network station addresses with which the highlighted DLC station address is associated. If there are more than 21 stations, the analyzer generates the message, "`xx network stations associated with this DLC station (first 21 shown below).`"

In Figure 4–47, since the DLC station, "BIZ-ONE," is a server, it transfers data for many network stations (leading its DLC address to be associated with a multitude of network station addresses. For an illustration of this concept, see Figure 4–40 on page 4–51). However, if the highlighted DLC station were a workstation, the **Associated network stations** list would probably include only the workstation itself.

Additional Token Ring Counters in the DLC Station Statistics Window

On token ring, the DLC Station Statistics window provides the following additional information:

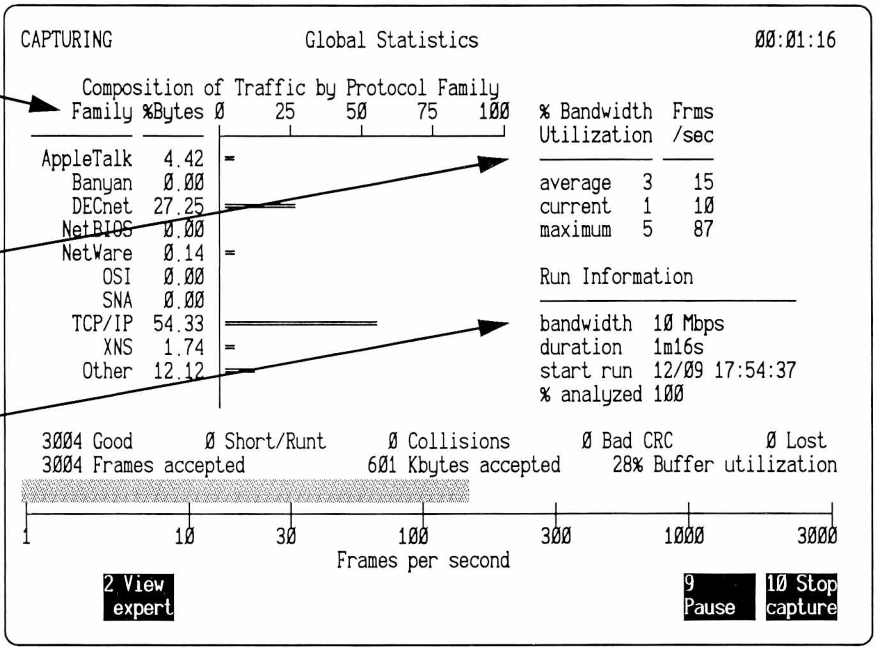
Station status — This field tells you whether the highlighted station is currently ON RING or OFF RING.

Upstream neighbor — Identifies the highlighted station's upstream neighbor by address or symbolic name.

Additionally, the DLC Stations Statistics window tabulates ring purge frames and informs you if the highlighted station is the active monitor.

The Global Statistics Window

The Global Statistics window provides a comprehensive percentage breakdown by protocol family of the traffic found on your network, as well as information about the current capture session. The information in the Global Statistics window is not immediately related to the investigation of symptoms and diagnoses; however, it does provide valuable insight on the types of traffic found on your network. Figure 4–48 shows the Global Statistics window for an Ethernet network.



```
CAPTURING                         Global Statistics                          00:01:16

       Composition of Traffic by Protocol Family
        Family %Bytes 0      25      50      75     100   % Bandwidth  Frms
                                                          Utilization  /sec
  AppleTalk   4.42 |-
     Banyan   0.00 |                                      average   3    15
     DECnet  27.25 |==========                            current   1    10
    NetBIOS   0.00 |                                      maximum   5    87
    NetWare   0.14 |=
        OSI   0.00 |                                      Run Information
        SNA   0.00 |
     TCP/IP  54.33 |====================                  bandwidth  10 Mbps
        XNS   1.74 |=                                     duration   1m16s
      Other  12.12 |====                                  start run  12/09 17:54:37
                   |                                      % analyzed 100

  3004 Good         0 Short/Runt        0 Collisions        0 Bad CRC        0 Lost
  3004 Frames accepted              601 Kbytes accepted       28% Buffer utilization

1            10        30          100          300          1000           3000
                                Frames per second
```

Percentage breakdown of network traffic by protocol family.

Percentage of total bandwidth utilization.

Information on current capture session.

Figure 4–48. The Global Statistics window.

The Global Statistics window is always available from the Expert Overview by using the F2 key. However, you cannot display the Global Statistics window from the various Expert subdisplays.

To display the Global Statistics window:

1. In the Expert Overview, notice the function key label F2 (**View stats**). Press F2.

   Result: The Global Statistics window appears, as in Figure 4–48.

   Note: After displaying the Global Statistics window, the function key label for F2 changes from **View stats** to **View expert**. You can use this key to toggle between the two views.

Composition of the Global Statistics Window

The Global Statistics Window consists of three categories of information:

- Composition of Traffic by Protocol Family
- Bandwidth Utilization

- Run Information

Each of these three categories is visible in Figure 4–48 and is described below.

Composition of Traffic by Protocol Family

The Expert analyzer dynamically tabulates all network traffic according to its protocol family. The results are presented both graphically (as a histogram) and as a numeric percentage. The thermometer-style horizontal bar allows you to see at a glance which count is increasing. The exact percentage of total traffic is displayed at the left end of the bar. For example, in Figure 4–48, TCP/IP traffic accounts for 54.33 percent of all network traffic, while AppleTalk accounts for only 4.42 percent.

How the Expert Analyzer Categorizes Packets into Protocol Families

In compiling the histogram, the expert system counts all the bytes in all the frames, except for the following.

1. Frames excluded by the capture filters.
2. Frames that arrive while capture is paused (F9 has been pressed).
3. Frames that are skipped because the expert analysis is unable to keep up with the influx of frames (in this case the "% analyzed" statistic, described below, will be less than 100%).
4. Internetwork analyzer only: FCS bytes, flag bytes and bits inserted by the bit-stuffing process.

Each frame is categorized into one of the protocol families listed at the left of the histogram. If none of the listed protocols apply, a frame is categorized as "Others". If more than one protocol applies, a frame is categorized according to the highest protocol analyzed.

For example, on a Frame Relay link, all traffic can technically be considered to be Frame Relay. However, encapsulated within most of these Frame Relay packets are LAN packets with higher-level protocols– for example, IP. The Expert analyzer would categorize all bytes in a Frame Relay packet with an encapsulated IP layer as part of the TCP/IP family. The only Frame Relay packets that the analyzer would categorize into the Frame Relay protocol family would be LMI frames, such as FECN and BECN frames. This convention lets you answer questions such as, "By how much would traffic be reduced if we removed all the TCP/IP stations from this network segment?"

Note: The expert system does not always parse to the highest layer of a frame. For example, the current software release will not recognize an AppleTalk frame that is encapsulated in a TCP/IP frame. Therefore it will categorize such a frame as TCP/IP rather than AppleTalk.

"Protocol Family" is a generic term for a related set of protocols. For example, the TCP/IP protocol family counter in the Global Statistics screen tabulates all protocols with an IP layer– not just TCP over IP. The other Protocol Families operate similarly.

Percentage Bandwidth Utilization

This category of counters measures the average, current, and maximum percentage of bandwidth used during the current capture session. **Current bandwidth usage** is measured over the interval of one second, on a "sliding-window" basis. That is, a new measurement is made every tenth of a second over the interval of one second (that is, measurements would be made from 1.0 to 2.0 seconds, from 1.1 to 2.1 seconds, and so on). **Maximum percentage of bandwidth** is the largest of these "current" bandwidth usage values. **Average bandwidth usage** is calculated by counting all frames that have entered the buffer since the start of the current capture and dividing this value by the total number of seconds the analyzer has been capturing frames (not paused).

Note: Although the analyzer makes many measurements per second, the counters are updated only once every second.

On the Sniffer Internetwork Analyzer (the Sniffer analyzer for WAN/Synchronous), the counts for percentage bandwidth utilization are expanded to measure **From DTE** and **From DCE** separately.

The **From DTE** and **From DCE** percentage bandwidth utilization counters are separate from one another. That is, they do not need to add up to 100 percent. Each WAN link consists essentially of two separate pipes with traffic travelling in opposite directions. Since each "pipe" is independent of the other, percentage bandwidth utilization could theoretically go to 100 percent for either one.

Additionally, there are statistics for average, current, and maximum number of packets per second. For example, in Figure 4–48, the maximum number of packets per second during this capture session was 87, while the maximum percentage of bandwidth utilization was five percent.

Run Information

The Run Information counters provide statistics about the current capture session as follows:

Bandwidth — The theoretical maximum amount of traffic that could travel over the network being analyzed. For example, the Bandwidth counter for Ethernet is 10 Mbps. For networks that do not have an established theoretical maximum (such as WANs) the analyzer can use a variety of algorithms to "figure out" the theoretical maximum.

Duration — The length of time between the first frame accepted into the analyzer's capture buffer during the current capture session and the most recent frame accepted into the capture buffer. The Duration counter is incremented each time a new frame is accepted into the buffer. The increment is based on the elapsed time between the accepted frame and the previous frame.

The Elapsed time counter (in the upper right corner of the display) simply keeps a running total of the time elapsed since capture was started. Whereas the Elapsed time counter has an upper limit of 99:59:99 (100 hours), the Duration counter will measure accurately up to a maximum period of 42 days.

There will sometimes be some discrepancy between the Duration counter and the Elapsed time counter in the upper right corner of the display. This can happen for the following reasons:

- When capture is paused, the Elapsed time counter does not increment. However, the Duration counter is measuring real time since the first frame was accepted. Therefore, when capture is resumed, the Duration counter will jump ahead to where it is higher than the Elapsed time counter. The amount of time the Duration counter is greater than the Elapsed time counter will be equal to the amount of time capture was paused.
- Under heavy traffic loads, the clock may be slow as the analyzer devotes more processing time to incoming traffic. As the analyzer catches up, the clock will be updated.

Start run

The time and date the current capture session was begun.

Note: The time and date correspond to those that the PC regards as current. If the PC's time and date are incorrect, the analyzer's will be as well. You can use the DOS commands `Time` and `Date` to change the time and date the PC regards as current.

% Analyzed

Because the amount of data passing over a network segment is potentially huge, the Expert analyzer will sometimes develop a backlog of frames waiting to be analyzed. The **% Analyzed** counter details how much of the data from the current capture session has been analyzed. During heavy traffic loads, this counter may fall below 100 percent. When capture stops, the analyzer will continue to perform Expert analysis until all unanalyzed frames still in the capture buffer have been processed.

Note: Under heavy traffic loads, the Expert will sometimes skip frames, never performing Expert analysis on them. At the end of a capture session, the **% Analyzed** counter indicates the percentage of total frames (that is, those seen during the current capture session) analyzed, giving you an idea of how many frames the Sniffer "saw" but was unable to analyze.

Effects of Capture Filters on Global Statistics

The statistics in the Global Symptoms window are based solely on those frames that reach the capture buffer. If you have set capture filters (such as protocol filters, station address filters, or destination class filters), various frames that do not pass these filters will never reach the capture buffer. Accordingly, the Expert analyzer's Global Statistics will not take these frames into account. This can render the Expert's statistics inaccurate.

This is particularly misleading in the case of the capture filters for protocols. For example, if in a DECnet environment you set a capture filter to exclude all DRP frames, the Expert analyzer will falsely report that some inordinately small percentage of your network traffic is DECnet. To ensure accurate statistics, you should set capture filters carefully.

Effects of Frame Size Option on Global Statistics

The **Frame Size** option allows you to specify (in bytes) what portion of each frame is passed into the capture buffer by the Expert analyzer. You can elect to "slice" frames after 32, 64, 128, 256, and 512 bytes. Frame slicing exists to boost capture performance. However, because the Expert analyzer bases its Global Statistics solely on that data which is passed into the capture buffer, frame slicing can cause inaccurate statistics in the Global Statistics window.

Generally, the Expert analyzer needs the first 128 bytes of each frame to compile accurate Protocol Family statistics. If **Frame Size** is set lower than 128 bytes, inaccurate Protocol Family statistics will result. To ensure accurate Protocol Family statistics, you will want to set the **Frame Size** option to **Whole frame** (the default).

Expert Display Filters

This section describes display filters that are specific to the Expert analyzer. Display filters determine which frames in the capture buffer will be displayed. Eliminating a frame from display with a display filter does not remove the frame from memory. Rather, it simply removes the frame from display. If the display filter eliminating a given frame from display were to be disabled, that frame would reappear. For a complete discussion of available display filters, see the *Distributed Sniffer System: Analyzer Operations Manual.*

This section describes the following Expert display filters:

- Network object display filter
- Symptom frames display filter

Network Object Filter

From the Expert window, you can determine what frames to include in the display. For example, you can include in the subsequent display only those frames that are related to a particular diagnosis or that are transmitted on a selected connection. This avoids cluttering up the display with frames that are irrelevant to the problem you want to investigate. The filtering is "automatic" because it does not require you to set up a filter as you normally would with the **Filters** option in the **Display** menu. Instead, you use the function key F2 (**Filter&disply**) to implement the **Network object** filter and determine the frames included for display.

The F2 key works as a toggle for setting and removing Network object filters. You cannot set a new **Network object** filter until you have cleared the existing one (unless, of course, there is no existing one).

The **Network object** filter does not remove frames from the capture buffer but omits them from the display. When some frames are skipped, the frames that remain visible have the same frame numbers as before. Thus, you may see frame 30 followed by frame 35 because the network object filter excludes frames 31-34.

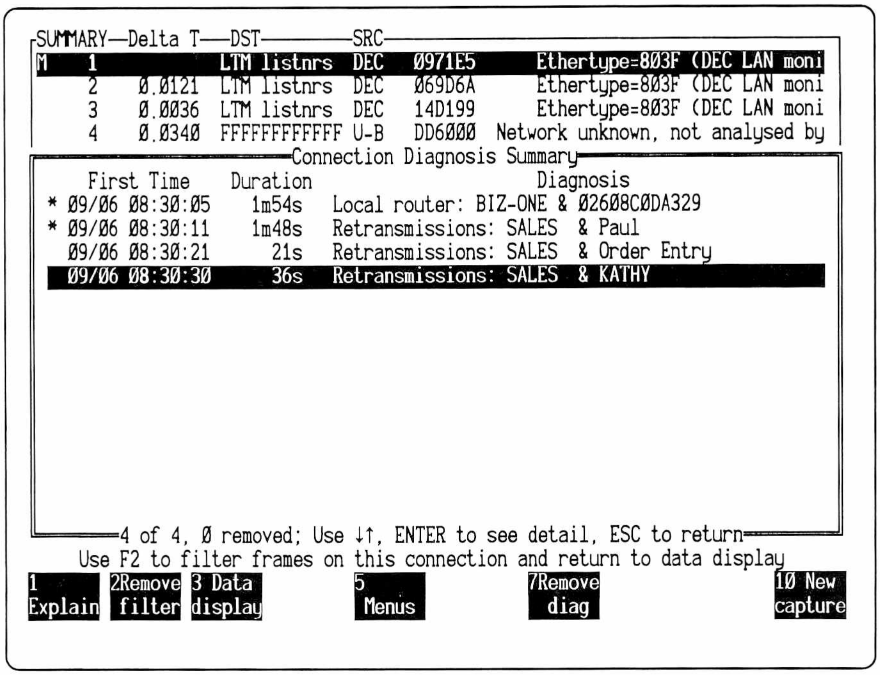
To set an automatic Network object filter:

1. Display the contents of the capture buffer in the Expert window.
2. The Expert window appears. Display an Expert Summary screen and highlight one of the following:
   - In a Diagnosis Summary screen, a diagnostic message at any layer.
   - In a Symptom and Network Object Summary window, a connection at the Application or Connection layers, or a station at the Network Station or DLC Station layers.

   The function key F2 (**Filter&disply**) appears at the bottom of the screen. Figure 4–49 shows the Diagnosis Summary screen at the Connection layer.

   Note: If a **Network object** filter is already set, you will have to clear the existing filter before setting a new one. The label for the function key F2 will indicate this by reading **Remove filter** rather than **Filter&disply.** See "Removing the Network Object Filter" on page 4–75 for more information.
3. Press F2 (**Filter&disply**).

   In response, the analyzer automatically filters out all frames irrelevant to the highlighted diagnosis, symptom, or network object, and takes you to the Classic window specified in the **Display** menu.

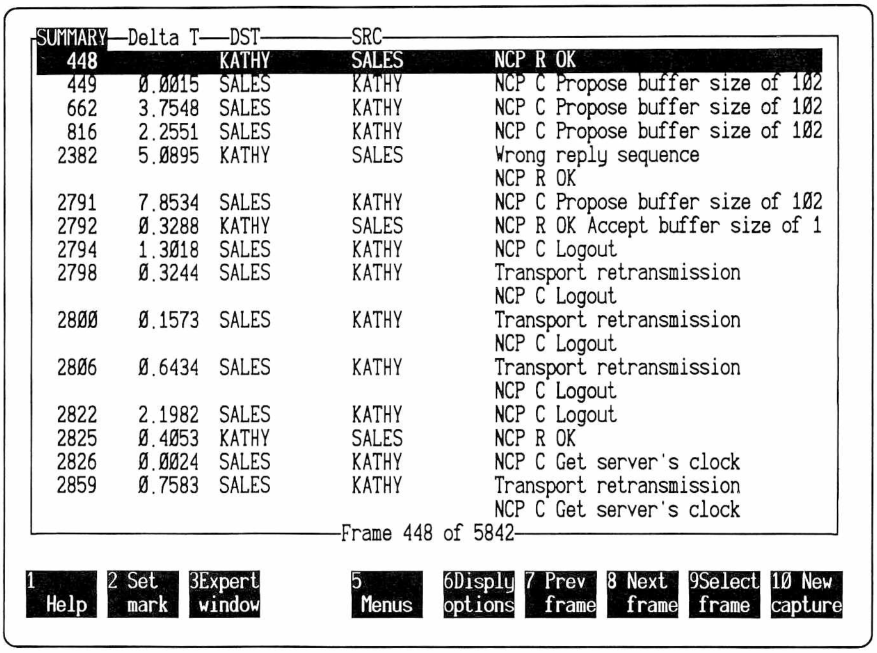


```
SUMMARY—Delta T——DST————————SRC——————————————————————————————
M    1             LTM listnrs  DEC   Ø971E5        Ethertype=8Ø3F (DEC LAN moni
     2     Ø.Ø121  LTM listnrs  DEC   Ø69D6A        Ethertype=8Ø3F (DEC LAN moni
     3     Ø.ØØ36  LTM listnrs  DEC   14D199        Ethertype=8Ø3F (DEC LAN moni
     4     Ø.Ø34Ø  FFFFFFFFFFFF U-B   DD6ØØØ  Network unknown, not analysed by
——————————————————Connection Diagnosis Summary————————————————————
     First Time      Duration                    Diagnosis
  * Ø9/Ø6 Ø8:3Ø:Ø5     1m54s   Local router: BIZ-ONE & Ø26Ø8CØDA329
  * Ø9/Ø6 Ø8:3Ø:11     1m48s   Retransmissions: SALES  & Paul
    Ø9/Ø6 Ø8:3Ø:21       21s   Retransmissions: SALES  & Order Entry
    Ø9/Ø6 Ø8:3Ø:3Ø       36s   Retransmissions: SALES  & KATHY

————————4 of 4, Ø removed; Use ↓↑, ENTER to see detail, ESC to return————————
     Use F2 to filter frames on this connection and return to data display
1       2Remove 3 Data        5              7Remove               1Ø New
Explain  filter display       Menus           diag                 capture
```

Figure 4–49. Setting a Network object filter. Notice the function key F2 .

Example: Setting a Network Object Filter

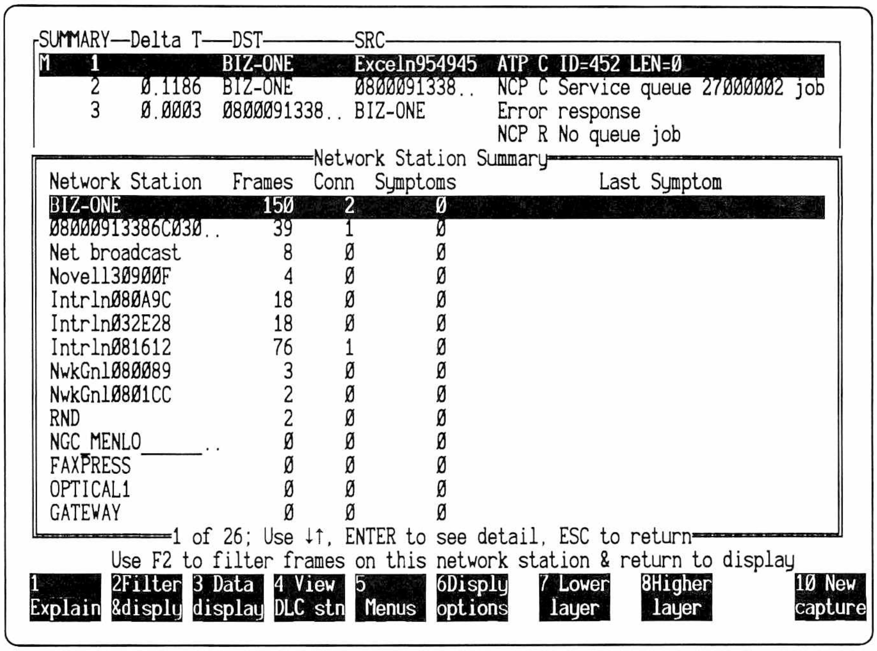
For example, in Figure 4–49 the analyzer has diagnosed four problems at the Connection layer. If you want to focus on the frames that are relevant to the highlighted diagnosis ("Retransmissions between SALES and Kathy"), highlight the diagnostic message. Then press F2 (**Filter&disply**) to display only those frames relevant to the highlighted diagnosis. The subsequent display is shown in Figure 4–50. Notice that the display starts with frame 448 and that the frame numbers are not contiguous. The displayed frames are the ones that lead to the diagnosis, "Retransmissions between SALES and Kathy."



```
SUMMARY—Delta T——DST————————SRC————————————————————————————————————————
  448              KATHY         SALES            NCP R OK
  449   0.0015     SALES         KATHY            NCP C Propose buffer size of 102
  662   3.7548     SALES         KATHY            NCP C Propose buffer size of 102
  816   2.2551     SALES         KATHY            NCP C Propose buffer size of 102
 2382   5.0895     KATHY         SALES            Wrong reply sequence
                                                  NCP R OK
 2791   7.8534     SALES         KATHY            NCP C Propose buffer size of 102
 2792   0.3288     KATHY         SALES            NCP R OK Accept buffer size of 1
 2794   1.3018     SALES         KATHY            NCP C Logout
 2798   0.3244     SALES         KATHY            Transport retransmission
                                                  NCP C Logout
 2800   0.1573     SALES         KATHY            Transport retransmission
                                                  NCP C Logout
 2806   0.6434     SALES         KATHY            Transport retransmission
                                                  NCP C Logout
 2822   2.1982     SALES         KATHY            NCP C Logout
 2825   0.4053     KATHY         SALES            NCP R OK
 2826   0.0024     SALES         KATHY            NCP C Get server's clock
 2859   0.7583     SALES         KATHY            Transport retransmission
                                                  NCP C Get server's clock
——————————————————————————————Frame 448 of 5842————————————————————————
```

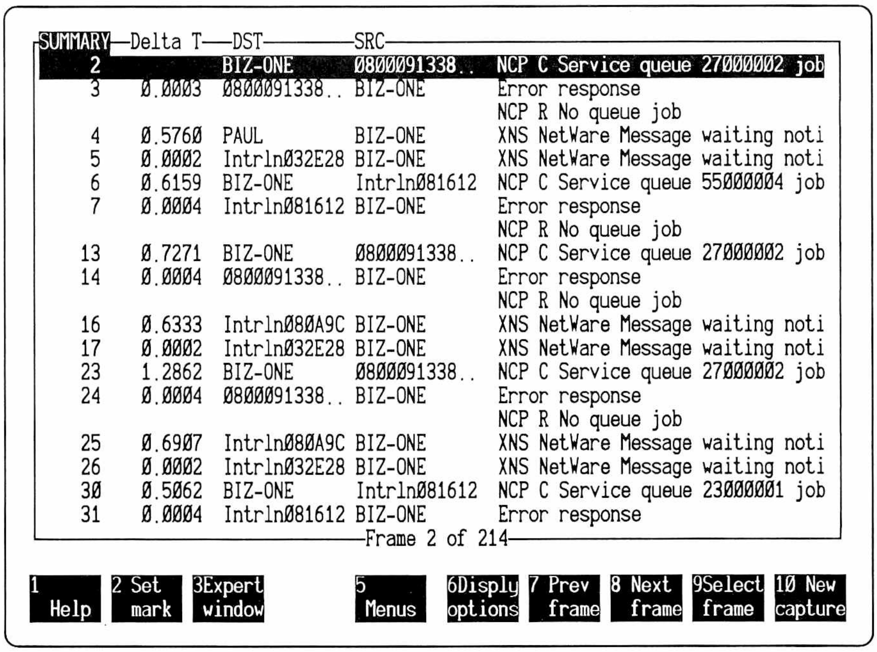
Figure 4–50. Summary display after Network object filter has been set on the diagnosis, "Retransmissions between SALES and Kathy."

The **Network object** filter lets you zero in on a particular diagnosis or symptom. However, you can also filter frames on any network object that interests you, whether or not the object has associated symptoms. For example, you can display the Network Stations Summary screen, as shown in Figure 4–51. To see all the frames to and from the server "BIZ-ONE," highlight the server's name and press F2 (**Filter&disply**). The Classic window shown in Figure 4–52 appears, containing all the frames to and from BIZ-ONE on its two connections.



```
SUMMARY—Delta T——DST————————SRC——————————————————————————————————
M    1                BIZ-ONE     Exceln954945  ATP C ID=452 LEN=0
     2     0.1186     BIZ-ONE     0800091338..  NCP C Service queue 27000002 job
     3     0.0003     0800091338.. BIZ-ONE      Error response
                                                NCP R No queue job
                    Network Station Summary
 Network Station     Frames  Conn  Symptoms          Last Symptom
 BIZ-ONE                150    2        0
 08000913386C030..       39    1        0
 Net broadcast            8    0        0
 Novell30900F             4    0        0
 Intrln080A9C            18    0        0
 Intrln032E28            18    0        0
 Intrln081612            76    1        0
 NwkGnl080089             3    0        0
 NwkGnl0801CC             2    0        0
 RND                      2    0        0
 NGC MENLO______..        0    0        0
 FAXPRESS                 0    0        0
 OPTICAL1                 0    0        0
 GATEWAY                  0    0        0
          1 of 26; Use ↓↑, ENTER to see detail, ESC to return
      Use F2 to filter frames on this network station & return to display
```

Figure 4–51. Network Stations Summary window. Notice the Classic Summary display in the background.



```
SUMMARY—Delta T——DST————————SRC——————————————————————————————————
     2                BIZ-ONE     0800091338..  NCP C Service queue 27000002 job
     3     0.0003     0800091338.. BIZ-ONE      Error response
                                                NCP R No queue job
     4     0.5760     PAUL        BIZ-ONE       XNS NetWare Message waiting noti
     5     0.0002     Intrln032E28 BIZ-ONE      XNS NetWare Message waiting noti
     6     0.6159     BIZ-ONE     Intrln081612  NCP C Service queue 55000004 job
     7     0.0004     Intrln081612 BIZ-ONE      Error response
                                                NCP R No queue job
    13     0.7271     BIZ-ONE     0800091338..  NCP C Service queue 27000002 job
    14     0.0004     0800091338.. BIZ-ONE      Error response
                                                NCP R No queue job
    16     0.6333     Intrln080A9C BIZ-ONE      XNS NetWare Message waiting noti
    17     0.0002     Intrln032E28 BIZ-ONE      XNS NetWare Message waiting noti
    23     1.2862     BIZ-ONE     0800091338..  NCP C Service queue 27000002 job
    24     0.0004     0800091338.. BIZ-ONE      Error response
                                                NCP R No queue job
    25     0.6907     Intrln080A9C BIZ-ONE      XNS NetWare Message waiting noti
    26     0.0002     Intrln032E28 BIZ-ONE      XNS NetWare Message waiting noti
    30     0.5062     BIZ-ONE     Intrln081612  NCP C Service queue 23000001 job
    31     0.0004     Intrln081612 BIZ-ONE      Error response
                                  Frame 2 of 214
```

Figure 4–52. Network object filter on the server BIZ-ONE.

Limitations of the Network Object Filter

The **Network object** filter has two limitations, listed below:

- Some symptoms and diagnoses, such as Broadcast storm, have no associated network object on which the analyzer can filter. In those cases, the F2 function key label will not appear at the bottom of display, indicating that a **Network object** filter cannot be set.
- Occasionally you may set a **Network object** filter on an object that no longer has associated frames in the capture buffer. In that case, the message "`No frames are eligible for display`" will appear.

For example, the analyzer may detect a connection between Agnes and the server BIZ-ONE at the beginning of a capture session. After capture has proceeded for several hours, capture is paused, and a **Network object** filter is set on that connection. While the analyzer knows that connection took place, the actual transmitted frames have been pushed out of the capture buffer by newer data. To ensure that the data you are interested in remains in the capture buffer, use a capture filter, or a trigger.

Note: The "`No frames are eligible for display`" message can also appear when the highlighted object has never actually sent or received a frame. For example, in the Network Stations Summary screen in Figure 4–51, if you highlight OPTICAL1, pressing F2 (**Filter&disply**) does not cause any filtering because OPTICAL1 has neither sent nor received frames.

Other Notes About the Network Object Filter

The Expert analyzer uses several algorithms to decide which frames are associated with the network object chosen as a filter. Sometimes, these algorithms may eliminate frames you consider relevant. For example, if you set a network object filter on a Novell Netware connection layer connection, the Expert analyzer would show all those related frames with NCP layers, but possibly would eliminate from display some connection maintenance frames that it considers irrelevant.

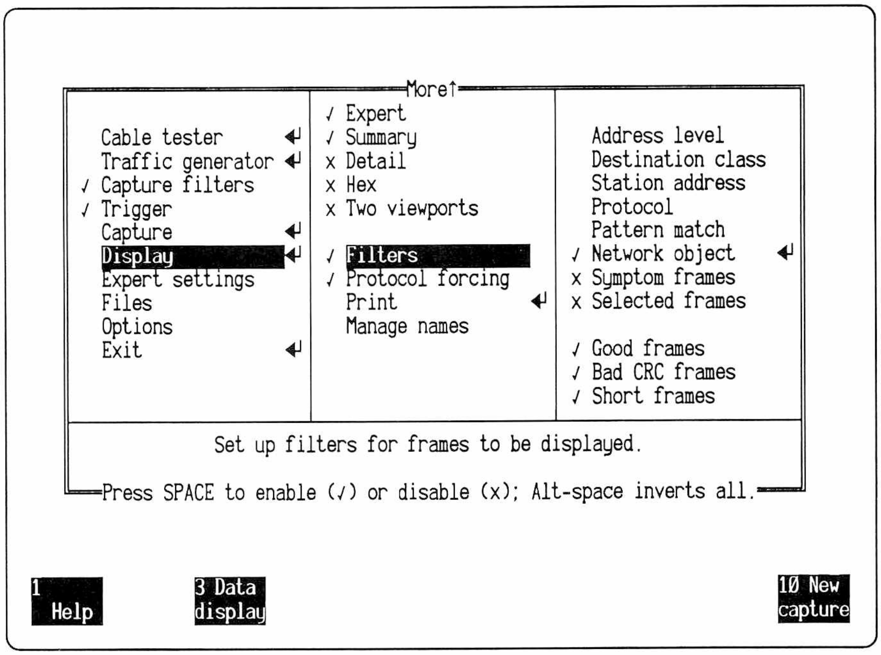
Displaying the Network Object Filter

The Expert analyzer allows you to view the network object on which it is filtering at any time.

To display the current Network object filter:

1. Move to **Display\Filters**.

   The display in Figure 4–53 appears.



```
                              More↑
                       ✓ Expert
  Cable tester      ↵  ✓ Summary               Address level
  Traffic generator ↵  x Detail                Destination class
✓ Capture filters      x Hex                   Station address
✓ Trigger              x Two viewports         Protocol
  Capture           ↵                          Pattern match
  Display           ↵  ✓ Filters             ✓ Network object  ↵
  Expert settings      ✓ Protocol forcing    x Symptom frames
  Files                  Print           ↵   x Selected frames
  Options                Manage names
  Exit              ↵                        ✓ Good frames
                                             ✓ Bad CRC frames
                                             ✓ Short frames

              Set up filters for frames to be displayed.

  Press SPACE to enable (✓) or disable (x); Alt-space inverts all.
```

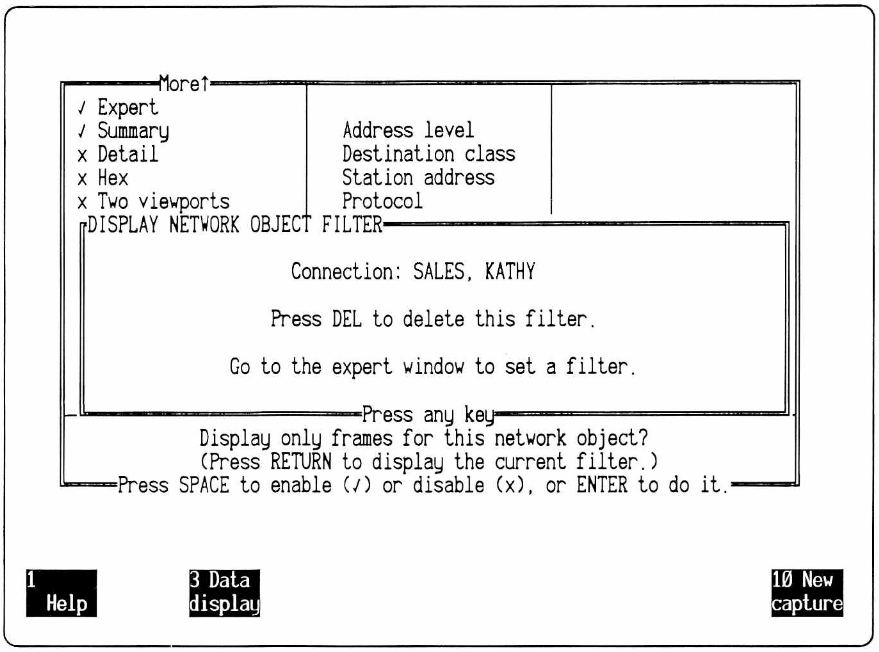
Figure 4–53. The Display \ Filters menu.

2. Move to **Network object** and press Enter.

   The analyzer displays the object on which the analyzer is currently filtering. Figure 4–54 shows a **Network object** filter on the connection between the two network stations, SALES and Kathy. Only frames associated with this connection will be displayed under the current **Network object** filter.

Note: If no **Network object** filter is currently set, the analyzer will display the message:

```
No Network object filter has been set.

Go to the Expert window to set a filter.
```



```
 More↑
✓ Expert
✓ Summary                 Address level
x Detail                  Destination class
x Hex                     Station address
x Two viewports           Protocol
DISPLAY NETWORK OBJECT FILTER

                 Connection: SALES, KATHY

               Press DEL to delete this filter.

            Go to the expert window to set a filter.

                        Press any key
           Display only frames for this network object?
            (Press RETURN to display the current filter.)
   Press SPACE to enable (✓) or disable (x), or ENTER to do it.
```

Figure 4–54. Displaying the current Network object filter.

Removing the Network Object Filter

Existing **Network object** filters must be removed before you can set a new one. **Network object** filters can be removed in two ways:

- Using the F2 (**Remove Filter**) function key. The function key F2 acts as a toggle for setting and removing **Network object** filters. This is the preferred method.
- Using the **Network object** filter menu item in the Display/Filters menu.

For information on setting a new filter, see "To set an automatic Network object filter:" on page 4–69.

To remove a Network object filter using the Network object menu item:

1. Move to **Display\Filters\Network object** and press Enter.

   The display in Figure 4–54 appears.

2. Press the Delete key to remove the current **Network object** filter.

Temporarily Disabling the Network Object Filter

Once a **Network object** filter is set, you may want to temporarily disable it without having to reset it later. In Figure 4–53, notice that the menu entry for the **Network object** filter is preceded by a √. By using the spacebar to toggle the √ to an x, you can temporarily disable the **Network object** filter without removing it.

To temporarily disable or enable a Network Object filter:

1. Move the highlight to the **Display\Filters** menu.

   The menu in Figure 4–53 appears.

2. Move to **Network object** and press Spacebar to change the √ to an x.

3. Press F3 (**Data display**) to display all frames in the capture buffer according to currently enabled filters.

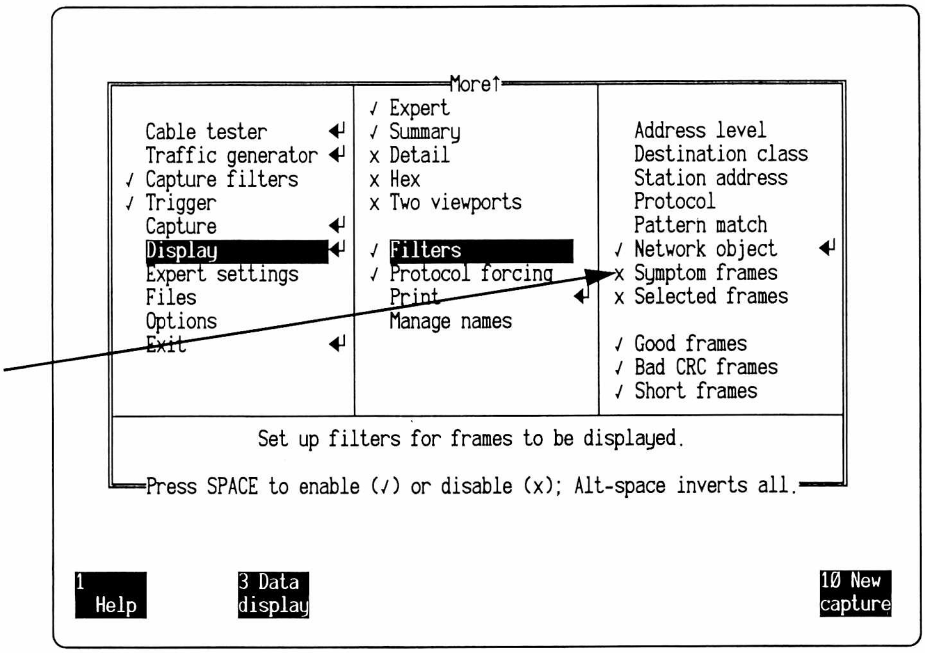
   Note: When you set a Network object filter, the filter is automatically enabled. If the Network object filter was disabled when you set it, a pop-up window will inform you that the filter has been enabled.

Symptom Frames Filter

In addition to the **Network object** display filter, the Expert analyzer also provides a **Symptom frames** display filter. The Symptom frames display filter allows you to filter from display those frames that do not exhibit symptoms. In this way you can filter a huge capture buffer down to just those frames that interest you.

To filter out frames that do not exhibit symptoms:

1. Move to **Display\Filters\Symptom frames.**



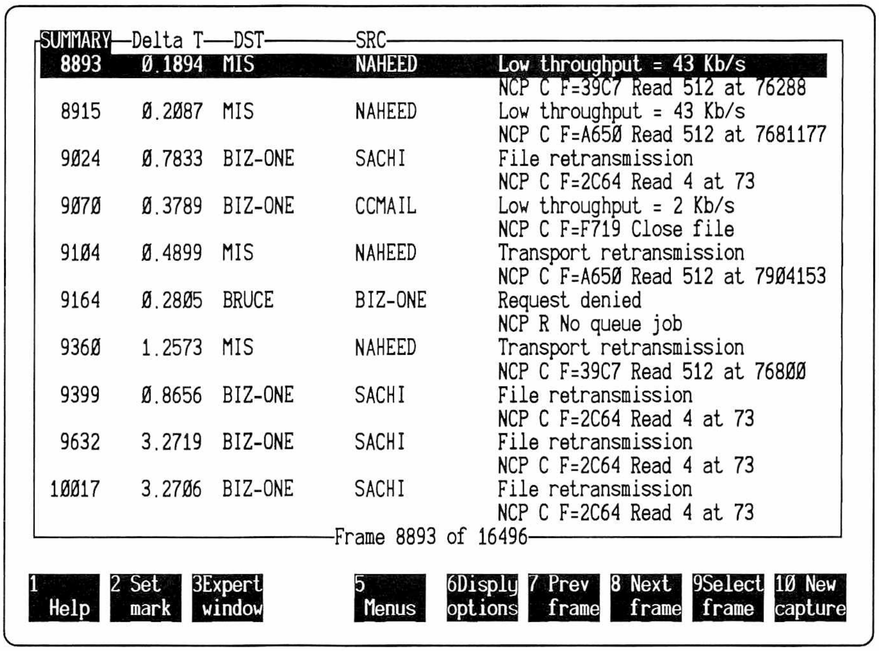
```
                          More↑
                      ✓ Expert
  Cable tester     ↵  ✓ Summary              Address level
  Traffic generator ↵ x Detail               Destination class
✓ Capture filters     x Hex                  Station address
✓ Trigger             x Two viewports        Protocol
  Capture          ↵                         Pattern match
  Display          ↵  ✓ Filters            ✓ Network object   ↵
  Expert settings     ✓ Protocol forcing   x Symptom frames
  Files                 Print           ↵  x Selected frames
  Options               Manage names
  Exit             ↵                       ✓ Good frames
                                           ✓ Bad CRC frames
                                           ✓ Short frames

                  Set up filters for frames to be displayed.
   Press SPACE to enable (✓) or disable (x); Alt-space inverts all.

1 Help        3 Data display                              10 New capture
```

Symptom frames filter

Figure 4–55. Symptom frames filter. Notice the x preceding the filter.

2. Press Spacebar to change the x in front of **Symptom frames** to a √, to enable the **Symptom frames** filter.

3. Press F3 (**Data display**) to display only those frames that exhibit symptoms. Figure 4–56 is an example of the Summary window after the **Symptom frames** filter was enabled.



```
SUMMARY—Delta T—DST————————SRC——————————————————————————————————————————
 8893   Ø.1894  MIS         NAHEED        Low throughput = 43 Kb/s
                                          NCP C F=39C7 Read 512 at 76288
 8915   Ø.2Ø87  MIS         NAHEED        Low throughput = 43 Kb/s
                                          NCP C F=A65Ø Read 512 at 7681177
 9Ø24   Ø.7833  BIZ-ONE     SACHI         File retransmission
                                          NCP C F=2C64 Read 4 at 73
 9Ø7Ø   Ø.3789  BIZ-ONE     CCMAIL        Low throughput = 2 Kb/s
                                          NCP C F=F719 Close file
 91Ø4   Ø.4899  MIS         NAHEED        Transport retransmission
                                          NCP C F=A65Ø Read 512 at 79Ø4153
 9164   Ø.28Ø5  BRUCE       BIZ-ONE       Request denied
                                          NCP R No queue job
 936Ø   1.2573  MIS         NAHEED        Transport retransmission
                                          NCP C F=39C7 Read 512 at 768ØØ
 9399   Ø.8656  BIZ-ONE     SACHI         File retransmission
                                          NCP C F=2C64 Read 4 at 73
 9632   3.2719  BIZ-ONE     SACHI         File retransmission
                                          NCP C F=2C64 Read 4 at 73
1ØØ17   3.27Ø6  BIZ-ONE     SACHI         File retransmission
                                          NCP C F=2C64 Read 4 at 73
————————————————————————Frame 8893 of 16496——————————————————————————————
```

Figure 4–56. Classic Summary display with ***Symptom frames*** *filter enabled.*

Advanced Navigation Techniques

This section describes several advanced techniques for navigating through the Expert window. As you grow more comfortable working with the Expert analyzer, these techniques will speed your work with the analyzer. They include:

- **Higher layer/Lower layer** function keys
- **Next symptom/Previous symptom** function keys

Using the Higher Layer/Lower Layer Function Keys

During post-capture display (or, while capture is paused), there are also several function keys available which allow you to trace the displays relating to a specific network object through the four Expert layers without having to return to the Expert Overview. For example, you could use the **Lower layer** key to trace the displays relating to a particular application from the Application layer down to the DLC Station layer. This eliminates the need to return to the Expert Overview before investigating related displays at another layer.

The **Higher layer/Lower layer** function keys are not available while the analyzer is actively capturing frames. They are available only while capture is paused or during post-capture display.

To use the Higher layer/Lower layer function keys:

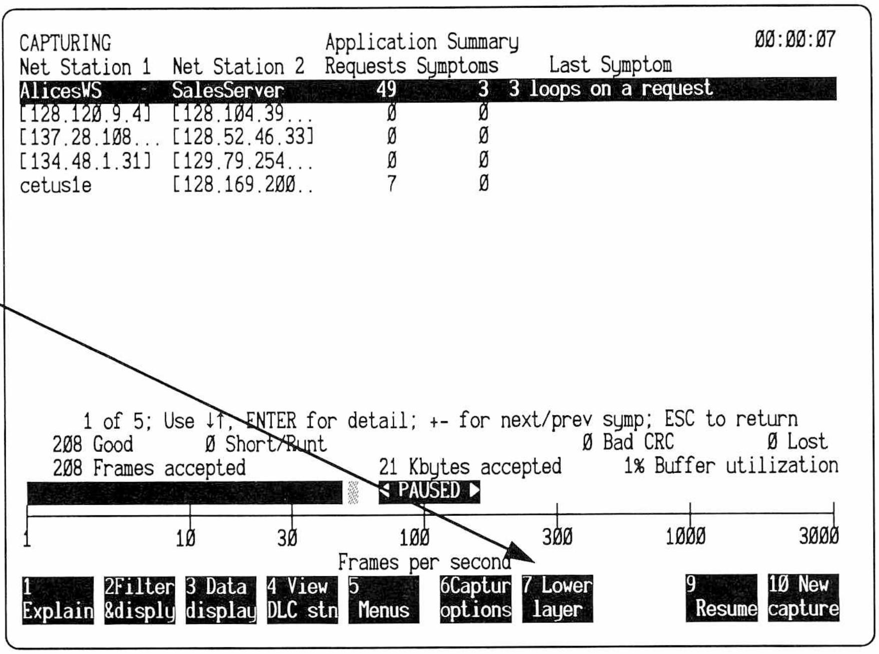
1. In a Summary, Detail, or Statistics window at any of the four Expert layers, use the cursor keys to highlight the application, connection, network station, or DLC station of interest.

2. If the analyzer is capturing frames, pause capture by pressing F9.

   Result: Additional key labels appear for F7 (**Lower layer**) and F8 (**Higher layer**) (Figure 4–57).

   Note: The F7 (**Lower layer**) and F8 (**Higher layer**) keys will appear only during post-capture display, or if capture is paused.

   Note: If the highlighted object is at the Application layer, the key label for F8 (**Higher layer**) will not appear, because there is no higher layer. Similarly, the key label for F7 (**Lower layer**) will not appear if the highlighted object is at the DLC Station layer because there is no lower layer.



```
CAPTURING                 Application Summary                          00:00:07
Net Station 1  Net Station 2  Requests Symptoms    Last Symptom
AlicesWS    -  SalesServer         49         3  3 loops on a request
[128.120.9.4]  [128.104.39...      0          0
[137.28.108... [128.52.46.33]      0          0
[134.48.1.31]  [129.79.254...      0          0
cetus1e        [128.169.200..      7          0


   1 of 5; Use ↓↑, ENTER for detail; +- for next/prev symp; ESC to return
 208 Good        0 Short/Runt                          0 Bad CRC         0 Lost
 208 Frames accepted               21 Kbytes accepted     1% Buffer utilization
                                  ◀ PAUSED ▶
1          10      30         100         300        1000        3000
                         Frames per second
```

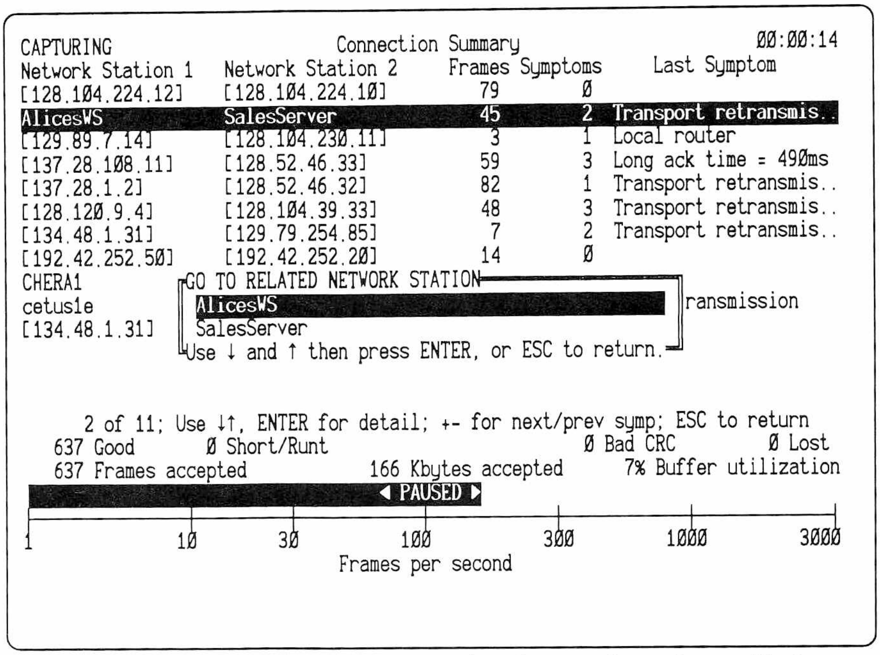
F7 (Lower layer) label appears when capture is paused or during post-capture display.

Figure 4–57. Application Summary screen with F7 (Lower layer) visible.

3. Press F7 (**Lower layer**) or F8 (**Higher layer**).

   Result: The object related to the highlighted object appears at the higher or lower layer, depending on which key was pressed. For example, if the highlight was on the application between the two stations **AlicesWS** and **SalesServer** (as in Figure 4–57) and F7 (**Lower layer**) was pressed, the display would now show the Connection Summary window with the corresponding connection highlighted (as in Figure 4–58).

   Note: If F7 (**Lower layer**) is pressed from a Connection layer Summary or Detail window, the pop-up box in Figure 4–58 appears. Because there are two network stations associated with a connection, the analyzer prompts you to select which of the two related network stations you want to see highlighted in the Network Stations window.



```
CAPTURING                    Connection Summary                       ØØ:ØØ:14
Network Station 1   Network Station 2   Frames Symptoms     Last Symptom
[128.1Ø4.224.12]    [128.1Ø4.224.1Ø]      79        Ø
AlicesWS            SalesServer           45        2  Transport retransmis..
[129.89.7.14]       [128.1Ø4.23Ø.11]       3        1  Local router
[137.28.1Ø8.11]     [128.52.46.33]        59        3  Long ack time = 49Øms
[137.28.1.2]        [128.52.46.32]        82        1  Transport retransmis..
[128.12Ø.9.4]       [128.1Ø4.39.33]       48        3  Transport retransmis..
[134.48.1.31]       [129.79.254.85]        7        2  Transport retransmis..
[192.42.252.5Ø]     [192.42.252.2Ø]       14        Ø
CHERA1          ┌GO TO RELATED NETWORK STATION═══════════════╗
cetus1e         │ AlicesWS                                   ║ransmission
[134.48.1.31]   │ SalesServer                                ║
                └Use ↓ and ↑ then press ENTER, or ESC to return.═╝

      2 of 11; Use ↓↑, ENTER for detail; +- for next/prev symp; ESC to return
   637 Good          Ø Short/Runt                      Ø Bad CRC          Ø Lost
   637 Frames accepted                166 Kbytes accepted      7% Buffer utilization
                                     ◀ PAUSED ▶
1             1Ø       3Ø         1ØØ          3ØØ          1ØØØ          3ØØØ
                              Frames per second
```

Figure 4–58. Pop-up box for selecting related network station to display.

Using the Next Symptom/Previous Symptom Keys

You can also use the + (**Next symptom**) and - (**Previous symptom**) keys to speed your navigation of the Expert window. These keys allow you to skip automatically between network objects that have symptoms associated with them. These keys are available in any of the displays accessible from the Objects/Symptoms column of the Expert Overview. They are available during capture, while capture is paused, and post-capture.

The **Next symptom/Previous symptom** keys are particularly valuable in the Detail and Statistics windows. You can use them to scroll automatically to the Detail or Statistics window for the previous/next network object with associated symptoms. This eliminates the need to return to the Summary view to find a network object with associated symptoms.

To use the Next symptom/Previous symptom keys:

1. In any display accessible from the Objects/Symptoms column of the Expert Overview, press + (**Next symptom**) or - (**Previous symptom**).

   Result: The display for the next or previous (depending on which key was pressed) object which has associated symptoms appears. The display corresponds to the display from which F2/F3 was pressed. Detail windows will appear from Detail windows, Statistics windows will appear from Statistics windows, and so on.

2. Note: If there are no previous symptoms and - (**Previous symptom**) is pressed, nothing will happen. Similarly, if there are no later symptoms and + (**Next symptom**) is pressed, nothing happens.

Function Keys in the Expert Window

This section describes the various function keys available in the Expert window. Different Expert displays have different associated function keys.

During Capture:

+/- The plus and minus keys allow you to move display to the next or previous symptom respectively.

F2 From the Expert Overview, pressing the F2 key displays the Global Statistics window.

F4 In the Summary displays, the F4 key allows you to change the format of the current Expert window. The available formats for the Summary window are described on page 4–40.

F7/F8 In the Diagnosis Summary and Diagnosis Detail windows, the F7 and F8 keys allow you to temporarily remove and restore diagnoses from the display. See page 4–12 for more information.

In displays accessible from the Objects/Symptoms column of the Expert Overview, F7 moves display to the next higher layer associated with the highlighted object, while F8 moves to the next lower layer associated with the highlighted object.

F9 F9 pauses capture temporarily. While capture is paused, the following additional function keys become available:

F10 F10 stops capture and returns you to the Main Menu of the analyzer.

While Capture is Paused

+/- The plus and minus keys allow you to move display to the next or previous symptom respectively.

F1 F1 provides a context-sensitive Explain message, displaying important information about the highlighted symptom or diagnosis.

F2 In the Expert Overview, pressing the F2 key displays the Global Statistics window.

In a Summary or Detail display, the F2 keys acts as a toggle for setting and removing **Network object** filters. For more information on **Network object** display filters, see the sections beginning on page 4–68.

F3 F3 acts as toggle between the analyzer's Expert and Classic display windows.

F5 F5 takes you to the analyzer's main menu.

F6

F6 provides a menu of Capture-related options.

F7/F8

In the Diagnosis Summary and Diagnosis Detail windows, the F7 and F8 keys allow you to temporarily remove and restore diagnoses from the display. See page 4–12 for more information.

In displays accessible from the Objects/Symptoms column of the Expert Overview, F7 moves display to the next higher layer associated with the highlighted object, while F8 moves to the next lower layer associated with the highlighted object.

F9

F9 resumes a paused capture.

F10

F10 starts a new capture.

APPENDIX A: SYMPTOM AND DIAGNOSIS MESSAGES A

Appendix A. Symptom and Diagnosis Messages

Overview

This appendix lists all the symptom and diagnosis messages generated by the Expert analyzer, and provides a brief description. The messages are grouped by Expert layers; within each layer, they are arranged alphabetically.

This appendix is not intended to provide detailed descriptions of each symptom and diagnosis. When the analyzer generates a symptom or diagnosis you do not understand, you should pause capture and press F1 to invoke a context-sensitive Explain message. Explain messages provide detailed descriptions for all the symptoms and diagnoses generated by the Expert analyzer including related thresholds and possible solutions to network problems.

Symptoms

Application Layer

File retransmission

An entire file, or a subset of a file has been retransmitted. This differs from a transport layer retransmission because the application is purposely retransmitting the file. Each retransmission is counted as a separate symptom.

Loops on same request

The application process on one station sent out the same request even though it has already received the appropriate reply from the destination station. Only requests that are sent within the time specified by **Filter time** are considered "repeated."

Low throughput/Slow file transfer

The rate of throughput during a file transfer was less than the minimum rate specified by the **Local transfer** or **Remote transfer** threshold. Throughput is measured for consecutive bytes within the same file.

Read/write overlap

Read or write requests to a file overlapped each other. For example, if an application wrote bytes 50 through 700, and then wrote bytes 200 through 800, there would be a write overlap because bytes 200-700 were written twice.

Request denied

The number of denied application requests exceeded the **Denied count** threshold. An application request is only counted as denied if it occurs within the time specified by **Filter time**. For more information, see "Denied Count" and "Filter Time" on page 3–18.

Connection Layer

Ack missing

A REPLY-ACK frame was expected but none was received.

Ack number decreasing

An acknowledgment specifies the segment number of the next octet to be received. The segment number points to the octet's position in the data stream. The amount of data accumulated by the receiver determines what the next octet should be. For example, if octets 1 through 5000 have been received, the receiver specifies the next octet to be 5001. As the transmission progresses, the segment number should increase. A decreasing number causes the sender to send an octet that has already been received. If the analyzer detects this situation, it displays this symptom message.

Ack wrong frame

A REPLY-ACK frame was seen as a response to a REQUEST-DATA frame; REPLY-ACK should only be seen as a response to a REQUEST-DATA-LAST frame.

Bouncing frames

The same frame has appeared twice, but with a decreasing value in the "time-to-live" field. This usually occurs between two routers or gateways, when the same packet is sent between two network stations repeatedly.

Command retransmission

A LAT command frame has been retransmitted. The analyzer tracks the exact number of command frames retransmitted.

Data sent while flow control off

A DECnet data frame was sent while flow control was turned off at the receiving station.

Fast retransmission

A retransmission occurred within less than the time specified by the **Fast retrans** threshold.

Refer to "Fast Retransmission" on page 3–22 for more information on this threshold and the related symptoms and diagnoses.

Flow control off for *x* seconds

DECnet flow control was turned off for *x* seconds, which exceeded the threshold specified by **Zero window**.

Idle more than *xx*

No communications were detected between the two end-points of a connection at the transport layer for more than the time specified by the **Idle timer** threshold.

Refer to "Idle Timer" on page 3–21 for more information on this threshold and the related symptoms and diagnoses.

Long ack time

The time that it took the receiver to acknowledge an octet was excessive. The analyzer uses an internal algorithm to determine the threshold. If the threshold is exceeded, it prints the symptom message. The threshold is 3 times the average acknowledgment time plus the **Fast retrans** threshold.

Missing reply

In a request/reply-based protocol (such as Novell PEP), a request was detected, but a corresponding reply was not detected.

Multiple source routing

In a token ring environment, a source-routed packet can be sent from one station to another using multiple paths. This is probably due to incorrect configuration of the token ring bridges.

NFS retransmission

An NFS request has been retransmitted. This is detected by comparing the current RPC transaction identifier with the previous value for this connection.

Packets too close

Two LAT frames are closer than 20ms. The LAT standard is 80ms.

Receive/Continue missing

A RECEIVE-CONTINUE frame was expected as a response to a REQUEST-DATA frame but a different frame was received instead.

Reply retransmission

A LAT reply frame has been retransmitted. The LAT standard states that retransmissions should not occur until at least one second has elapsed from the prior transmission.

Synchronization frame missing

A SYNC frame was expected but none was received.

Transport retransmission

The sequence number is less than or equal to its previous value, indicating that this frame contains data that has already been transmitted.

Window frozen

The TCP window size of the highlighted station has been stuck for longer than the time specified by the **Zero window** threshold.

Window size exceeded

In a windowed protocol (such as TCP or DECnet), the sender sent a segment that contained more data than the receiver's advertised window size.

Wrong reply sequence

The reply sequence number did not match the request sequence number.

Zero window

The TCP window size of the highlighted station has been zero for longer than the duration specified by the threshold **Zero window**.

Network Station Layer

The symptoms and diagnoses at the network layer are concerned with addressing and how traffic is routed from the local network to remote networks.

Destination unreachable

The highlighted station has sent or received *x* number of ICMP "destination unreachable" messages.

Duplicate net address

The same network address was mapped to more than one DLC address.

Improper DECnet address

The first four bytes of a DECnet network layer address should always be AA000400. This symptom is generated if a non-conforming address was found in a Long Data or an endnode hello packet.

ICMP error

The highlighted station has received an ICMP message indicating a parameter problem.

Inconsistent server advertisement

Two routers advertise a Novell server with a hop count of one. This hop count value for a Novell SAP means that a router is the server.

Inconsistent subnet mask

The subnet mask specified in an ICMP "address mask reply" message did not match any of the expected subnet masks. The subnet mask could be legitimate, but it is not specified in the STARTUP.ENV file. Use the **Set subnet mask** utility in the **Expert settings** menu to edit subnet masks.

IP fragment missing

An IP layer fragment on an NFS connection has been lost. This will usually result in an NFS layer retransmission.

IP fragment out of order

An IP layer fragment on an NFS connection was not in sequential order.

Local router

When the analyzer detects that a router is routing traffic between two local stations, it displays a symptom message. Because the stations are located on the same network, no routing should be necessary.

Many routers to remote

A local station can connect to a remote station through more than one router on the local network.

Multiple routers to local station

The number of routers used to gain access to a local station has equalled or exceeded the **Multiple Routers** threshold.

Network unreachable

The highlighted station has received an ICMP "network unreachable" message.

Port unreachable

The highlighted station has sent an ICMP "port unreachable" message. The message indicates that the station has received a frame sent to the named port, but the port cannot be accessed by the receiving station.

Redirect network/host/frame

The highlighted station has sent an ICMP "redirect host" message. Routers send these messages to inform stations of better routes to desired destinations.

Small hello timer

The rate of DECnet endnode hellos is smaller than the **DEC Hello** threshold. A high rate of DECnet hellos contributes unnecessarily to network overhead.

Source address is broadcast

The source address in a packet is a broadcast address.

Source quench

The highlighted station has received an ICMP "source quench" message. Source quench messages inform stations to reduce their rate of frame transmission.

Time-to-live exceeded

The highlighted station has received an ICMP "Time Exceeded" message. The time-to-live field of the IP layer has reached zero, and therefore the frame has been discarded.

Time-to-live expiring

An IP frame has been detected with a "time-to-live" field equal to 1 or 0, indicating that the frame is about to expire.

Zeros broadcast address

Lists the number of IP frames sent from the highlighted station to an all-zero broadcast address.

DLC Station Layer

Broadcast storm

The rate of broadcast frames sent on the network has exceeded the **Broadcast sy** threshold.

Frame not analyzed

One or more frames were not analyzed by the Expert analyzer. This may happen during heavy network traffic. If the frames are still in the capture buffer, you can overcome this by reanalyzing the data in the capture buffer.

Frame too short

A frame fragment has been detected. The fragment is shorter than the DLC address fields.

LAN overload

The network data rate used a greater percentage of available bandwidth than that specified by the **LAN overload** threshold.

Physical level error

The analyzer has detected a physical level error. If the number of physical errors per second exceeds the **Physical error** threshold, the analyzer will generate a diagnosis. Physical errors include short frames, frames with bad CRCs, and lost frames.

Source DLC address is broadcast

The source DLC address field is a broadcast address.

MAC Layer (Token Ring)

The analyzer captures and reports all MAC level frames on the token ring. Since MAC level frames are essential for troubleshooting token rings, the analyzer reports most MAC frames as symptoms.

Abort error

An "abort delimiter transmitted" MAC condition has been detected.

AC error

The next active upstream neighbor is unable to set the Frame Copied/Address Recognized bits in a frame it has copied.

Bad FC/AR flags

The analyzer has detected an invalid format in the Frame Copied/Address Recognized bits of a frame from the highlighted station.

Burst error

There is a signaling error in the cable. The error is not caused by a station entering or leaving the ring. The Expert analyzer filters out those Burst error frames caused by ring entry and departure.

Duplicate test successful

The Duplicate Address Test MAC frame has been successful (another station on the ring has the same address). When the DLC address of a station trying to enter the ring is the same as the DLC address of a station already in the ring, the station attempting entry is automatically disconnected.

Excessive ring purge

The number of ring purge frames has exceeded the **Rng purge sy** threshold in the **Expert settings** menu.

Frame relay buffer depth exceeded

The buffer depth on the router has exceeded a preconfigured threshold. Frames may be lost as a result. If possible, the router should be reconfigured with more buffers.

Internal error

The highlighted station has a recoverable internal error. If the station is reporting multiple internal errors, the station is marginal.

Line error

A "line error" MAC condition has been detected. There was an invalid character in a frame or token, or there was a check error in a frame.

Local node with route designator

Source routing is being used but the source and destination stations are both on the same local ring.

Multiple local ring definitions

Source routing is being used. The routing information in two or more frames is contradictory-- that is, two frames have different definitions of the local ring number.

New active monitor

There is a new active monitor on the ring.

Receiver congestion error

The analyzer has detected a Receiver congestion MAC frame. Receiver congestion occurs when a station does not have enough room in its buffer to copy a frame for which it is the destination. If the number of Receiver congestion MAC frames per second exceeds the **RX Congestion** threshold, a diagnosis is generated.

Returned to ring

The highlighted station has reentered the ring, after having left the ring. A new symptom is generated each time the station reenters the ring.

Ring beaconing

The highlighted station has transmitted a Beacon MAC frame in an attempt to bring the ring back into normal operation. Also a diagnosis.

Station off ring

The highlighted station has left the ring, either purposely or due to a ring problem. A new symptom is generated each time the station leaves the ring.

Token error

The token has been lost. This error should only be generated by the active monitor when it recognizes the need to create a new token.

WAN/Synchronous

DISC frame

One or more DISC (disconnect) frames have been received. The HDLC link has been disconnected and must be reestablished before any data transfer can proceed. All previous connections must be renewed.

DLCI bandwidth exceeded

Frame Relay symptom. The measured bandwidth exceeds the requested bandwidth reported in the most recent local management interface (LMI) PVC status frame. The requested bandwidth is the amount guaranteed by the Frame Relay service. It is legal to exceed this amount occasionally, but most Frame Relay services do not guarantee full frame delivery if the value is exceeded.

DLCI keepalive sequence error

Frame Relay symptom. The sequence number in a keepalive LMI frame has been reset to zero. Frames may have been lost immediately prior to this occurrence.

Excessive backward congestion

Frame Relay symptom. The percentage of frames with the Backward Explicit Congestion Notification (BECN) bit set exceeds the **Congestion %** threshold in the **Expert settings\Thresholds** menu.

The BECN bit indicates backward congestion on a Frame Relay link. The BECN bit is set by a congested network to notify the user that congestion avoidance procedures should be initiated in the opposite direction of the transmitted frame.

Excessive forward congestion

Frame Relay symptom. The percentage of frames with the Forward Explicit Congestion Notification (FECN) bit set exceeds the **Congestion %** threshold in the **Expert settings\Thresholds** menu.

The FECN bit indicates backward congestion on a Frame Relay link. The FECN bit is set by a congested network to notify the user that congestion avoidance procedures should be initiated in the opposite direction of the transmitted frame.

FRMR frame

One or more FRMR (frame reject) frames have been received. FRMR frames indicate an error condition not recoverable by retransmission. Investigate the FRMR frames for more details about the cause of each error.

HDLC retransmission

One or more HDLC numbered information frames have been retransmitted.

Inappropriate SABM

An HDLC SABM (set asynchronous balanced mode) frame has been received, but the Modulo 128 encoding option is currently selected in the **Options** menu of the Sniffer analyzer. This is an inconsistency. You should select the Modulo 8 encoding option instead. Encoding options are found in the **Options** menu of the Sniffer analyzer.

Inappropriate SABME

An HDLC SABME (set asynchronous balanced mode extended) frame has been received, but the Modulo 8 encoding option is currently selected in the **Options** menu of the Sniffer analyzer. This is an inconsistency. You should select the

Modulo 128 encoding option, instead. Encoding options are found in the **Options** menu of the Sniffer analyzer.

Inappropriate SNRM

An HDLC SNRM (set normal response mode) frame has been received, but the **Frame type** option in the Sniffer analyzer's **Options** menu is not currently set to **SDLC then SNA**. Because the HDLC SNRM frame is usually seen only on an SNA network, you should probably set the **Frame type** option to **SDLC then SNA**.

REJ frame

A REJ (reject) frame has been received. This usually indicates that one or more frames have been lost. If this happens often, check your modem and line for correct operation.

Router buffer overflow

Frame Relay symptom. The buffer depth on the router has exceeded a preconfigured router threshold, possibly causing frames to be lost. If possible, the router should be reconfigured with more buffers.

WAN underload

The Expert analyzer generates the WAN underload symptom when the data rate falls below the percentage of available bandwidth specified by the **WAN underload** threshold in the **Expert settings** menu.

WAN congested

The Expert analyzer generates the WAN overcongested symptom when the data rate exceeds the percentage of available bandwidth specified by the **WAN overload** threshold in the **Expert settings** menu.

Diagnoses

Application Layer

Excessive requests denied

This diagnosis indicates that a server has denied an excessive number of application requests relative to the number of successful requests. The related threshold is **Denied request %**.

Refer to "Excessive Requests Denied" on page 4–18 for more information on this diagnosis.

File overlap/retransmission

This diagnosis indicates that the same block of a file is retransmitted between two stations too many times.

When the analyzer counts the number of retransmissions, it also includes the number of file overlaps. Refer to "File Overlap / Retransmission" on page 4–19 for more information on this diagnosis.

Slow file transfer

The analyzer generates the **Slow file transfer** diagnosis when the ratio of slow versus normal file transfers is greater than the **Slow file %** threshold in the Expert settings menu. The analyzer uses different thresholds depending on whether frames were routed locally or remotely.

Refer to "Slow File Transfer" on page 4–33 for more information on this diagnosis and the related thresholds.

Slow server

This diagnosis indicates that the analyzer considers the highlighted server slow because of the time it takes for it to respond to application requests.

Refer to "Slow Server" on page 4–34 for more information on this diagnosis and its related thresholds.

Connection Layer

Non-responsive station

The analyzer generates this diagnosis when the number of consecutive identical retransmissions without response on a given connection exceeds the **No responses** threshold in the **Expert settings** menu.

Refer to "Non-Responsive Station" on page 4–29 for more information on this diagnosis and related thresholds.

Retransmissions

The analyzer generates this diagnosis when the number of retransmitted frames on a given connection (expressed as a percentage of good transmissions versus retransmissions on the connection) exceeds the **Retransmission percentage** threshold in the Expert settings menu.

Refer to "Retransmissions" on page 4–31 for more information on this diagnosis and related thresholds.

Network Station Layer

Duplicate network address

The analyzer generates this diagnosis (and symptom) when two or more DLC stations are associated with the same network address.

Refer to "Duplicate Network Address" on page 4–16 for more information on this diagnosis and related thresholds.

Local router

The analyzer generates this diagnosis when two DLC stations on the same network segment are communicating via two or more routers, rather than directly from one DLC station to the other.

Refer to "Local Router" on page 4–27 for more information on this diagnosis.

Multiple routers to station

The analyzer generates this diagnosis when there are more routers on the local network that can route frames to a remote station than specified by the **Multiple routers** threshold.

Refer to "Multiple Routers to Station" on page 4–28 for more information on this diagnosis and related thresholds.

DLC Station Layer

Broadcast/Multicast storm

The analyzer generates this diagnosis when the number of broadcast/multicast frames per second exceeds the rate specified by **Broadcast dg** in the **Expert settings** menu.

Refer to "Broadcast Storm" on page 4–15 for more information on this diagnosis and related thresholds.

LAN overload

The analyzer generates this diagnosis when the rate of network traffic in a given minute is too high. This depends on the settings of the thresholds **LAN overload** and **LAN overload percentage**.

Refer to "LAN Overloaded" on page 4–26 for more information on this diagnosis and the related thresholds.

High rate of physical errors

The analyzer generates this diagnosis when the rate of physical errors per second detected for a particular station exceeds the rate specified by the **Physical errors** threshold.

Refer to "High Rate of Physical Errors" on page 4–22 for more information on this diagnosis and its related threshold.

MAC Layer (Token Ring)

High rate of congestion

The analyzer generates this diagnosis when the rate of MAC receiver congestion errors per second exceeds the rate specified by the **RX Congestion** threshold.

Refer to "High Rate of Congestion" on page 4–20 for more information on this diagnosis and its related threshold.

High rate of line/burst errors

The analyzer generates this diagnosis when the rate of MAC level line plus burst errors for a given station exceeds the **Ring errors** threshold.

Refer to "High Rate of Line or Burst Errors" on page 4–21 for more information on this diagnosis and its related threshold.

High rate of remove from ring requests

The analyzer generates this diagnosis when the rate of MAC level remove from ring requests sent to a given station exceeds the **Stn removed** threshold.

Refer to "High Rate of Remove from Ring Requests" on page 4–23 for more information on this diagnosis and its related threshold.

High rate of ring entries

The analyzer generates this diagnosis when the rate of MAC level ring entries from a given station exceeds the **Ring entries** threshold.

Refer to "High Rate of Ring Entries" on page 4–24 for more information on this diagnosis and its related threshold.

High rate of ring purges

The analyzer generates this diagnosis when the rate of MAC level ring purge frames from a given station exceeds the **Rng purge dg** threshold.

Refer to "High Rate of Ring Purges" on page 4–25 for more information on this diagnosis and its related threshold.

Ring beaconing

The analyzer generates this diagnosis when it detects a MAC level ring beacon frame.

Refer to "Ring Beaconing" on page 4–32 for more information on this diagnosis and its related threshold.

WAN/Synchronous

WAN overloaded

The data rate has exceeded the threshold specified by the **WAN overload** threshold for longer than the duration specified by the **Overload timer** threshold.

Underloaded network

The data rate has fallen below the threshold specified by the **WAN underload** threshold for longer than the duration specified by the **Underload timer** threshold.

Refer to "Underloaded Network" on page 4–35 for more information on this diagnosis and its related thresholds.

INDEX

Network General

Index

Network General

We simplify network complexity.™

Network General Corporation
4200 Bohannon Drive
Menlo Park, California 94025
+1 (415) 473-2000

Network General Europe
Belgicastraat 4
1930 Zaventem , Belgium
+32 (2) 725-6030

Network General Canada, Ltd.
9225 Leslie Street, Unit #7
Richmond Hill, Ontario L4B 3H6 Canada
+1 (416) 882-7905

P/N:20103-001